SAFEBOOK 4

Allen-Bradley

Guardmaster®

マシンの安全関連制御システム

原理、規格、および実装

LISTEN. THINK. SOLVE.℠

Rockwell Automation

SAFEBOOK 4

マシンの安全関連制御システム

マシンの安全関連制御システム

目次

第1章　規定 2
EU指令および法規、機械指令、機械使用の指令、米国の事例、OSHA (米国労働安全衛生局)、カナダの規制

第2章　規格 18
ISO (国際標準化機構)、IEC (国際電気標準会議)、EN (欧州統一)規格、米国の規格、OSHA規格、ANSI規格、カナダの規格、オーストラリアの規格

第3章　安全ストラテジ 23
リスクアセスメント、機械の制限、タスクと危険の特定、リスクの見積もり、リスク低減、安全な設計、保護システムと保護措置、評価、トレーニング、個人用保護具、規格

第4章　保護手段および補助的な装置 35
接近の阻止、固定式保護ガード、接近の検出、安全のための製品とシステム

第5章　安全距離の計算 57
危険性がある可動部の安全制御に安全距離を利用するための計算式、利用方法の手引き、および適用

第6章　予期しない電源投入の回避 61
ロックアウト/タグアウト、安全遮断システム、負荷切断、トラップ・キー・システム、ロックアウトの代替手段

第7章　安全関連制御システム&機能安全 63
概要、機能安全とは何か、IEC/EN 62061およびEN ISO 13849-1:2008、SILおよびIEC/EN 62061、PLおよびEN ISO 13849-1:2008、PLとSILの比較

第8章　EN ISO 13849-1:2008に従うシステム設計 69
安全システムアーキテクチャ(構造)、活動時間、危険側故障発生までの平均時間($MTTF_d$)、自己診断率(DC)、共通原因故障(CCF)、系統的故障、安全遂行レベル(PL)、サブシステム設計および組合せ、妥当性確認、マシンの立上げ、フォルト排除

第9章　IEC/EN 62061に従うシステム設計 90
サブシステム設計 - IEC/EN 62061、プルーフテスト間隔の影響、共通原因故障の影響の分析、カテゴリからの移行方法、アーキテクチャによる制約、B10とB10$_d$、共通原因故障(CCF)、自己診断率(DC)、ハードウェア・フォルト・トレランス、機能安全の管理、単位時間当たりの危険側故障確率(PFH_D)、プルーフテスト間隔、安全側故障割合(SFF)、系統的故障

第10章　安全関連制御システムの構造に関する注意事項 101
概要、制御システムのカテゴリ、検出されないフォルト、コンポーネントおよびシステム定格、フォルトに関する注意事項、フォルト排除、IEC/EN 60204-1とNFPA 79に従う停止カテゴリ、米国の安全制御システムの要件、ロボット規格:米国およびカナダ

第11章　SISTEMAを使用するアプリケーション例 123
SISTEMA安全遂行レベルの計算ツールとロックウェル・オートメーションのSISTEMA製品ライブラリを共に使用する方法についてのアプリケーション例

Allen-Bradley

EU指令および法規

このセクションの内容は機械の安全性、特に保護システムのガードとインターロックに関与する人のためのガイドです。産業用設備の設計者およびユーザを対象としています。

ECおよびEFTA内にオープンマーケットの概念を普及させるために、そのメンバーであるすべての国々は、機械およびその使用に関する必須安全要求事項を定義する法律を制定する義務があります。

これらの要件を満たさない機械は、ECおよびEFTAの加盟国で販売したり、持ち込んだりできません。

産業用機械および装置の安全性に直接関与する欧州指令が2つあります。それは、以下の2つです。

1 機械指令

2 作業機器使用指令

機械指令の「健康と安全に関する必須要求事項(EHSR)」は、作業機器使用指令における装置の安全性を確認するために使用できるので、これら2つの指令は、直接関係していると言えます。

このセクションでは、この両方の指令の特長について取上げており、ECおよびEFTA加盟国で産業用設備の設計、供給、購入、使用に関与する人は、これらの指令の要件について十分理解していることが望まれます。機械のサプライヤとユーザの多くは、これらの指令に従わない限り、ECで活動することは絶対に許されません。

産業安全に関連する欧州指令は、使用中、準備中も含め、この他にもいくつか存在します。それらのほとんどは、用途別にかなり専門化されているので、このセクションでは取り上げていませんが、関連する場合は、その要件を満たす必要があるので、十分注意しなければなりません。例えば、次のような指令があります：
EMC指令2004/108/ECおよびATEX指令94/9/EC

EU機械指令

機械指令新しい機械および安全関連部品を含むその他の装置の供給を対象にしています。指令の条項や要件に従わずに、EU内にマシンを供給することは違法です。

指令内で使われている「機械」の最も広義の意義は以下の通りです：アセンブリ、人や動物の労力を直接利用しないドライブシステムに取付けたか取付けることを意図するもの、リンクされた部品やコンポーネントから構成されるもの、少なくとも1つの動くものがあるもの、および特定のアプリケーションのために互いに連結されているもの

マシンへのCEマーク認証

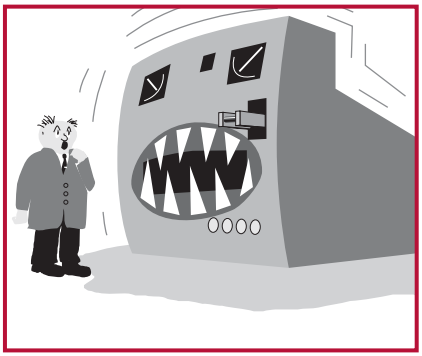
現在の機械指令(2006/42/EC)は、2009年の終わりに以前のバージョン(98/37/EC)と置き換わりました。明確にして改定していますが、「健康と安全に関する必須要求事項(EHSR)」を根本的に変更するものではありません。これは、技術と手段への変化を考慮して、いくつかの変更を行ないました。カバーする機器のタイプをさらに拡大しています(例：建設現場のホイスト)。そのため、どのEHSRが適合可能かを決定するためのリスクアセスメントの明確な要件と、付録IV機器についての適合性評価手順の変更を行なっています。

オリジナルの指令(98/37/EC)の重要な条項は、機械に対しては1995年１月1日に、安全関連部品に対しては1997年1月１日に完全な効力を発揮するようになりました。

現在の指令(2006/42/EC)の条項は、2009年12月29日に適用できるようになりました。供給される機器を確実に指令に適合させるのは、製造メーカまたはその正式な代表者の責任になります。これには、以下が含まれます。

- 指令の付属Iに含まれている適合可能なEHSRを満たしていることを確認
- 技術ファイルを準備
- 適切な適合性評価を行なう。
- 「EC適合宣言書」を提供
- CEマークを適合する場所に貼る。
- 安全に使用するための手順を提供

健康と安全に関する要件



指令の付録1には、該当する機械が従わなければならない健康と安全に関する要件(EHSRともいう)のリストが記載されています。このリストの目的は、機械が安全で、その機械の設計から廃棄に至る全段階において、人を危険に曝すことなく、使用、調整、メンテナンスを行なえるように設計および構築されていることを保証することにあります。以下に一般的な要件についての概要を示しますが、付録1に記載されたEHSRをすべて考慮することが重要です。

検討中にどのEHSRが機器に適合するかを判断するためにリスクアセスメントを実施する必要があります。

付録1のEHSRは、危険排除に関する対策の階層も設定しています。

(1) 本質安全設計：可能な限り、設計そのものであらゆる危険を回避します。

これが不可能な場合、**(2) 追加の保護装置**、例えば、アクセスポイントをインターロックするガード、ライトカーテンやセンサマットなどの無形バリアなどを使用する必要があります。

前述の手段で処理できない残留リスクは、**(3) 個人用保護具またはトレーニング**によって阻止する必要があります。機械のサプライヤは、何が適切かを指定する必要があります。

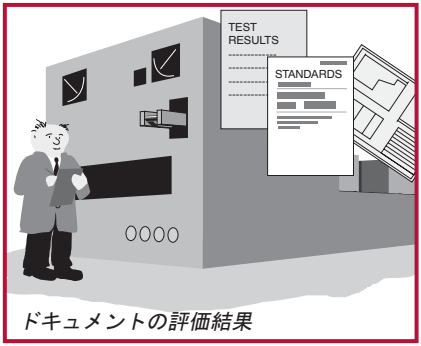
構造および操作には、適切な器具を使用する必要があります。十分な照明と取扱施設を用意する必要があります。制御機器および制御システムは、安全で信頼できなければなりません。機械は、突然始動することがあってはならず、1つ以上の非常停止装置を装備している必要があります。処理のアップストリームまたはダウンストリームが機械の安全性に影響する複雑な設備には、特別な配慮が必要です。電源装置や制御回路の傷害が危険な状況を引き起こすことは許されません。機械は安定性があり、予測可能なストレスに耐えられなければなりません。けがの原因となるエッジや表面の露出部分をなくす必要があります。

ガードや保護装置は頑強な構造で、通り抜けることが困難でなければなりません。固定式保護ガードは、工具の使用によってのみ解除できる方法で取付ける必要があります。可動式保護ガードは、インターロック機構を備えている必要があります。調整式保護ガードは、工具なしで簡単に調整できる必要があります。

電気およびその他のエネルギー供給事故を防ぐ必要があります。熱、爆発、騒音、振動、粉塵、ガス、または放射線による傷害のリスクを最小限に抑える必要があります。メンテナンスおよび点検に対する適切な準備が必要です。十分な表示機能および警告装置を用意する必要があります。機械には、設置、使用、調整などを安全に行なうための取扱説明書を添付します。

適合性評価

設計者または他の責任機関は、EHSRに準拠している証拠を示すことができなければなりません。このファイルには、テスト結果、図面、仕様などすべての関連情報が含まれます。



ドキュメントの評価結果

機械指令について欧州連合の官報(OJ)にリストされた欧州(EN)の統一規格と、適合性に対する仮定をなくした日付は、失効せず、特定のEHSRに適合するための仮定を協議します(OJにリストされた多くの最新の規格には、規格にカバーされたEHSRを探すためのクロスリファレンスが含まれている)。

装置が欧州の特定の統一規格に合わせて設計されている場合に、EHSRに対する適合性を示す作業が簡単になります。これらの基準は法律的には必要ありませんが、別の方法で適合性を証明することは、極めて複雑な課題になりうるので、これらの使用が強く推奨されます。これらの基準の構造は、ISOと連携するCEN (ヨーロッパ標準化委員会) およびIECと連携するCENELEC (ヨーロッパ電気標準化委員会)によって作成され、機械指令を支持しています。CENとCENELECとが一緒になって、ヨーロッパ標準化連合 (European Committee for Electrotechnical Standardization)を結成しています。

文書化された完璧なリスクアセスメントを実施することは、考えられるすべての機械の危険に対処できることを裏付けるために必要です。同様に、機械製造メーカには、欧州の統一規格で取り組まれていないことであってもEHSRをすべて確実に満たす責任があります。

技術ファイル

製造メーカまたは正式な代表者は、EHSRに準拠している証拠を示すために技術ファイルを順位する必要があります。このファイルには、テスト結果、図面、仕様などすべての関連情報が含まれます。

すべての情報が永続的にハードコピーとして利用可能であることは不可欠ではありませんが、所轄官庁(機械装置が適合していることを監視するためにEU各国から任命された機関)からの要請によって技術ファイル全体を閲覧可能にしておく必要があります。

少なくとも、以下の資料が技術ファイルに含まれていることが必要です。

1. 制御回路図を含む機器の全体図
2. 機械装置のEHSR適合性をチェックするために必要な詳細な図面、計算記録など
3. 機械装置に適用される必須健康安全要求のリストや、実装されている保護対策の説明を含むリスクアセスメントの資料
4 対象となる必須健康安全要求を示す、使用されている規格および他の技術仕様のリスト
5 機械装置が示す危険を除去するために採用される方法の説明
6 関連がある場合、試験施設またはその他の機関から取得された技術報告書や認定書
7 欧州の統一規格で適合を宣言する場合、そのテスト結果を示す技術報告書
8 機械装置の操作手順書のコピー
9 該当する場合は、半完成品の機械類が組み込まれていることの表明と、そのような機械類の関連組立て手順
10 該当する場合は、機械類または機械類に組み込まれているその他の製品の適合に関するEC適合宣言書のコピー
11 EC適合宣言書のコピー

量産する場合は、製造されたすべての機械装置が適合していることを保証するための内部基準の詳細(例えば品質管理システムなど)：

- 製造メーカは、コンポーネント、取付け部品、または完成機械類に対して必要な調査またはテストを実施し、機械類が安定して設置され安全にサービスを開始できるように設計され、組み立てられていることを確認します。
- 技術ファイルは、常に単一ファイルとして存在している必要はありませんが、必要な文書を適宜利用できるように1つのファイルにまとめることが可能でなければなりません。技術ファイルは、機械の最後のユニットの製造から10年間、利用可能であることが必要です。

機械類の製造に使用したサブアセンブリについては、EHSR適合を実証するために不可欠である場合を除いて、詳細な計画やその他の固有情報を技術ファイルに含める必要はありません。

付録IV機械の適合性評価

ある種の機器は、特殊な条例に制約されます。このような機器は指令の付録IVにリストされ、一部の木材加工機械、プレス機、抽出成形機、坑内機器、車両修理用リフトなどが含まれます。

また、付録IVには、人の存在を検出するように設計された保護装置(例えば、ライトカーテン)や、安全機能を保証するためのロジックユニットなどの一部の安全関連部品も含まれています。

欧州の統一規格に完全に適合したわけではない付録IVの機械に対しては、製造メーカまたは正式な代表者は、以下の手順のいずれかを行なう必要があります。

1. EC型式審査：技術ファイルを準備して、機械のサンプルをEC型式審査のために認定機関(テスト機関)に提出する必要があります。合格した場合、その機械には、EC型式審査証明書が与えられる。認定の妥当性のために、5年ごとに認定機関で再検討を受ける必要があります。
2. 完全な品質保証：技術ファイルを準備して、製造メーカは設計、製造、最終検査、およびテストするために認可された品質システムを動作する必要があります。品質システムは、この指令の条項について機械の適合性を保証する必要があります。

認定機関の検査

付録IVに含まれない機械、または付録IVに含まれているが関連する欧州の統一規格に完全に適合している機械については、製造メーカまたはその正式な代表者が技術ファイルを準備して機器の適合を評価して宣言することもできます。製造された機器の準拠を保証するには、内部チェック必要です。

認定機関

認定機関は、相互に連絡を取り合い、共通の基準で作業を行なうネットワークを、EU全体に張り巡らせています。認定機関は政府(産業ではなく)によって任命されており、認定機関の資格を持つテスト機関および研究所の詳細は、以下のWebサイトから入手できます。

http://ec.europa.eu/enterprise/sectors/mechanical/machinery/index_ en.htm

EC適合宣言の手順

CE 供給するすべての機械にCEマークを添付する必要があります。この機械は、CE適合宣言と共に供給されなければなりません。

CEマークは機械が適合可能なすべての欧州指令に準拠して、対応する適合性評価の手順が完了していることを示します。機械が関連するEHSRを満たしていない限りは、機械指令についてCEマークの適用は違法になります。

EC適合宣言書には、以下の情報が含まれていることが重要です。

- 製造メーカの商号と完全な住所、および該当する場合正式な代表者
- 技術ファイルを編集することを許可された人物の名前と住所。この人物はEU領域内にいる人物でなければなりません(EC領域外の製造者の場合は、「正式な代表者」の場合もある)。
- 機械類の説明とこれを特定するもの。これには、一般的な名称、機能、モデル、タイプ、シリアルナンバー、取引名などがあります。
- 機械類がこの宣言のすべての関連対応を満たしていることを表す文章、および該当する場合、他の指令への適合または機械類が適合している関連対応について宣言している類似の文章
- 該当する場合は、使用されている統一規格への参照
- 該当する場合は、使用されている他の技術規格および仕様への参照
- (付録IVの機械に対して)該当する場合、付録IXに記載されているECタイプの試験を実施した通知機関の名前、住所、およびID番号と、EC型式テストの認定証番号
- (付録IVの機械に対して)該当する場合、付録Xに記載されている完全な品質保証システムを承認した通知機関の名前、住所、およびID番号
- 宣言の場所と日付
- 製造メーカまたは正式な代表者にかわって宣言の作成に携わった人のIDと署名

半完成機械類に対するEC組込みの適合宣言書

後日他の品目と組み合わせて完全な機械を形成する機器が提供される場合、これに対して組込み適合宣言書を発行する必要があります。CEマークは適用しないでください。この宣言書には、当該機器を組み込んだ機械に対して適合が宣言されるまで、使用すべきでない旨を明記する必要があります。これについて、技術ファイルを用意する必要があり、また半完成機械類は、安全が損なわれないように、完成機械類へ正しく組み込むために満たすべき条件の説明を含む情報が添付されて提供される必要があります。

このオプションは、独立して機能する機器や、機械の機能を変更する機器には利用されません。

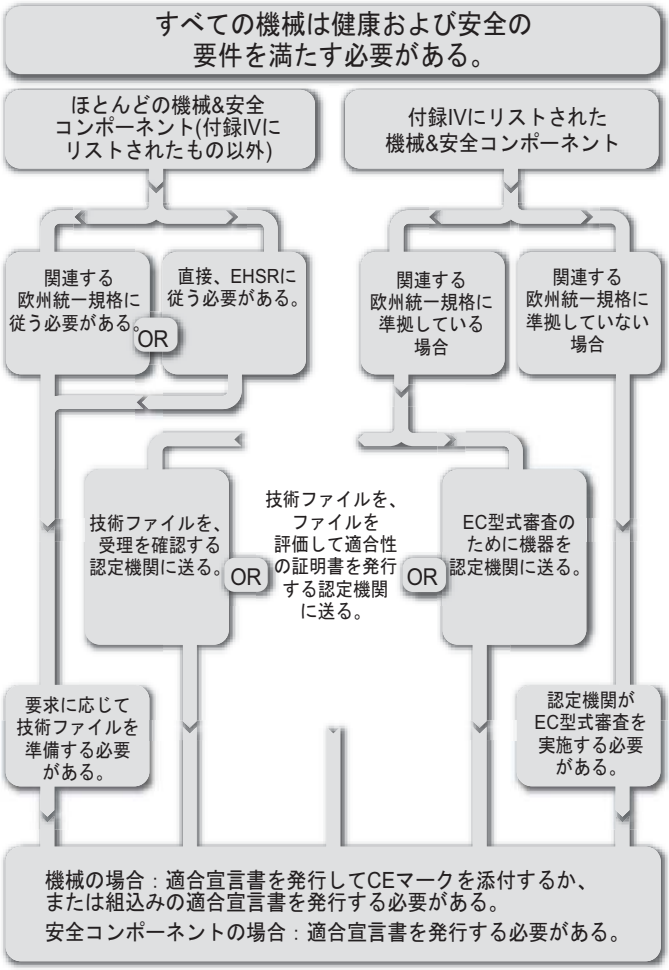
組込みの適合宣言書には、以下の情報が含まれていることが必要です。

- 半完成機械類の製造者の商号と完全な住所、および該当する場合は正式な代表者
- 関連する技術文書を編集することを許可された人物の名前と住所。この人物はEU領域内にいる人物でなければなりません(EC領域外の製造者の場合は、「正式な代表者」の場合もある)。
- 半完成機械類の説明とこれを特定するもの。これには、一般的な名称、機能、モデル、タイプ、シリアルナンバー、および取引名などがあります。
- この指令の中でどの重要な要件が適用され満たされているかということを宣言する文章と、付録VIIのBに従って関連技術文書が編集されたことを宣言する文章、および該当する場合、他の関連宣言と共に半完成機械類の適合を宣言する文章
- 国内当局の正当な求めに応じて、半完成機械類の関連情報の伝達を保証すること。これには伝達方法が含まれていて、半完成機械類の製造者の知的財産権を侵害しないような方法にすべきです。
- 該当する場合、半完成機械類を組み込んだ完成機械に対して、この指令の対応についての適合が宣言されるまで、当該機械類を使用すべきでない旨を示すステートメント
- 宣言の場所と日付
- 製造メーカまたは正式な代表者にかわって宣言の作成に携わった人のIDと署名

EU領域外から供給される機械 - 正式な代表者

EU (またはEEA)領域外に本拠地を置く製造メーカがEUに機械を輸出する場合は、正式な代表者を指名する必要があります。

正式な代表者とは、製造者から、製造者の代理として機械類の指令に関連した義務や手続きを実行するために、書面による指令を受領した、EC (欧州共同体)内にいる個人または法人を意味します。



機械指令に対する手順の概要

機械指令が供給者を対象としているのに対して、この指令(89/655/EECの95/63/ECによる改訂、2001/45/ECおよび2007/30/EC)は、機械の使用者を対象としています。すべての産業部門を対象としており、事業者が負うべき全般的な義務と、作業機器の最低限の安全要件を規定しています。すべてのEU諸国では、この指令を実施するために独自の法律を制定しています。すべてのEU加盟国は、この指令を実施するために、独自の形式で法規を制定しています。

例えば、英国では、作業機器の提供と使用規則(The Provision and Use of Work Equipment Regulations) (通常P.U.W.E.R.と略す)という名称で、番号が付けられた条例をまとめた形式で実施しています。実施方法は、国によって異なりますが、指令の効力は保持されます。

これらの規定は、この指令の対象となる装置の種類と仕事場について詳細に説明されています。

さらにこれらの規定は、安全な作業体系の制定や適切なメンテナンスが必要な適切で安全な機器の提供など、事業者に対する全般的な義務も規定しています。機械オペレータには、機械を安全に使用するために、正確な情報とトレーニングを提供する必要があります。

1993年1月1日以降に提供された新規の機械類(およびEU領域外から持ち込まれた中古機械類)は、機械指令など関連するすべての製品指令(暫定的な取決めに従う)を満たす必要があります。EU内から初めて作業場に持ち込まれた中古機器は、U.W.E.指令の付録に記載されている最低の要件をすぐに満たす必要があります。

注：大幅な修理や改造を行なった既存または中古の機械類は新規機器と分類されるので、これらの機器で実行される作業は、(自社内で使用する場合であっても)機械指令に準拠していることを確認する必要があります。

「作業機器の適合性」は、指令のもっとも重要な部分で、事業者の責任で(Management of Health and Safety at Work Regulations 1992に基づいて)、リスクアセスメントの適切なプロセスを実施することに焦点を当てています。

これは、機械類が適切にメンテナンスされている必要がある要件です。これは、通常、予防的メンテナンススケジュールを計画し、ルーチン化する必要があることを意味します。ログが集計されて最新のものが保持されていることが推奨されます。このことは、機器のメンテナンスや検査が保護装置や保護システムの安全性を維持するのに貢献している場合特に重要です。

U.W.E.指令の付録には、作業機器に適用される一般的な最小要件が指定されています。

機器が関連する製品指令(機械指令など)に適合している場合、これらの機器は付録の最低の要件に指定されている対応する機械設計要件に自動的に適合しています。

加盟諸国は、U.W.E.指令の最小要件を超える作業機器の使用に関する法律を発布することができます。

作業機器使用指令の詳細は、EUの公式サイトをご覧ください。

http://europa.eu/legislation_summaries/employment_and_social_policy/health_hygiene_safety_at_work/c11116_en.htm

米国の規制

ここでは、米国の産業用機械保護安全規格について紹介します。これは単に開始点にすぎません。ユーザはその特定のアプリケーションについての必要条件を更に明らかにし、その設計、使用方法、保守の手順や実情がユーザ自身の必要性のみならず国や地方の法令や規格に確実に適合するようにしなければなりません。

米国には産業安全を推進する多くの機関が存在し、これらには以下のようなものがあります。

1. 制定された必要条件とともに、独自の内部必要条件を設定している社団法人

2. 職業安全衛生管理局(OSHA)

3. 全国防火協会(NFPA)、ロボット協会(RIA)、および生産技術協会(AMT)といった産業組織、およびロックウェル・オートメーションのような安全製品およびソリューションのサプライヤ

OSHA (米国労働安全衛生局)

米国では、産業安全の主要な原動力の1つは、職業安全衛生管理局(OSHA)です。OSHAは、米国議会の決議によって1970年に設立されました。この法令の目的は、安全で健康的な作業環境を提供して、人材を保護することです。この法令は、企業に適用できる強制的な職業安全衛生規格を設定する権限を労働長官に付与したことで、州際通商にも影響を与えました。この法令は、米国、コロンビア特別区、プエルトリコ連邦、バージン諸島、米国領サモア、グァム、太平洋諸島信託統治領、ウェーク島、連邦大陸棚領域法で定義されている大陸棚、ジョンストン島、および運河地帯に存在する職場で行われる雇用に対して適用されます。

この法令の第5項では、基本的な必要事項を設定しています。すべての事業者は、その従業員の業務および作業場所に関して考えられる、死または重大な身体的危害に繋がる危険性を排除する設備を整えることで、この法令が定める職業安全衛生規格を満たす必要があります。

さらに、第5項では、すべての事業者が職業安全衛生規格、およびこの法令に従って発行された規則、規程、指令の中でそれぞれの活動および事業に適用されるものをすべて遵守するように述べています。

OSHA規格は事業者と従業員の両方に責任を課しています。これが機械指令との大きな相違点です。機械指令は、サプライヤに危険性のない機械の販売を義務付けています。米国では、サプライヤは安全装置のない機械を販売することができます。機械を安全に使用するために、ユーザが安全装置を取付ける必要があります。この規則が成立した時点ではこれが普通でしたが、機械が設計され、製造された後で安全装置を追加するよりも、安全性を考慮して機械を設計した方がはるかに低コストになるため、傾向としてはサプライヤが機械に安全装置を取付ける方が主流になっています。現在は、サプライヤとユーザが安全装置の必要事項について話し合うことで、機械をより安全にするだけでなく、生産性を向上させようという試みが一般的になされています。

マシンの安全関連制御システム

労働長官は、任意の国民的合意規格、および制定されている連邦法を、その規格が特定の従業員の安全および健康の改善に繋がらない場合を除き、職業安全衛生規格として公布できる権限を持っています。

OSHAでは、最終的にこの規格を連邦規則集第29編(29 CFR)で公開しました。産業機械に関連する規格は、OSHAにより29 CFR Part 1910で公開されています。これらの規格は、OSHAのWebサイト(www.osha.gov)で自由に参照できます。一般的な規格とは異なり、OSHA規格は自由意思によるものではなく、法規です。

機械安全に関する重要な項目を、以下に紹介します。

A - 総則

B - 確立した連邦の基準の採用および準用

C - 安全一般および健康に関する規定

H - 危険物

I - 個人用保護具

J - 環境管理(ロックアウト/タグアウトを含む)

O - 機械および機械の防護装置

R - 特殊な産業

S - 電気

一部のOSHA規格では、任意規格にも言及しています。参照文書として取り入れることには、連邦公報で全面的に公開されたものとして扱われるという法的効力があります。国民的合意規格がサブパートに参照文書として掲載された場合、その規格は法律と考えられます。例えば、NFPA70 (米国電気工事基準と呼ばれる任意規格)は、サブパートSに参照文書として掲載されています。これによって、NFPA70規格必須事項はOSHAでも必須になります。

サブパートJの29 CFR 1910.147では、危険な動力の管理について述べています。これは、通常ロックアウト/タグアウト規格と呼ばれます。これに相当する任意規格はANSI Z244.1です。基本的に、この規格では修理中またはメンテナンス中は、機械の電源をロックアウトするように規定しています。この目的は、意図せずに機械を出力状態にしたり、始動させたりすることで、従業員が負傷するのを回避することにあります。

事業者は適切なロックアウト装置またはタグアウト装置を取付けて、装置を絶縁したり、機械または装置が動作しないようにすることで、意図しない動作、始動または蓄積されたエネルギーの放出を回避して、従業員を事故から守るためのプログラムを確立し、手段を利用する必要があります。

通常の生産作業中に行なわれるツールの小規模な変更や調整、およびその他の小規模な修理作業は、定期的に繰返される、製造用装置の使用に不可欠な日常業務で、その作業が有効な保護機能を備えた代替手段を使用して行なわれるのであれば、この規格の対象外です。代替手段とは、ライトカーテン、セーフティマット、ゲートインターロック、およびその他安全システムに接続されている同等の装置など、安全保護装置を意味します。機械の設計者およびユーザの課題は、何が「小規模な」修理で、何が「日常的に繰返される不可欠な」作業かを判断することです。

サブパートOでは、「機械および機械の防護装置」について定めています。このサブパートには、すべての機械に関する一般的な必要事項だけでなく、一部の特殊な機械に関する必要事項のリストもあります。1970年にOSHAが設立されたとき、既存のANSI規格が多数取り入れられました。例えば、機械式パワープレスに関するB11.1は、1910.217として取り入れられました。

1910.212は、機械に関する一般的なOSHA規格です。ここでは、機械領域のオペレータやその他の従業員を、作業点、入り口のニップポイント、回転部品、飛沫や飛火によって発生する危険から保護するために、機械保護の手段を1つ以上装備するように指示しています。防護装置は、可能な場合は機械に取付け、何らかの理由で機械に取付けることが不可能な場合は他の場所に取付けます。ガードは、それ自体に事故危険性があってはなりません。

「作業点」とは、処理対象の原料に対して実際に作業が行なわれる機械の領域を意味します。機械の作業点では、作業者が危険に曝されることになるので、防護装置が必要です。ガードは、適切な規格に適合しているか、適用できる特定の規格がない場合は、作業中にオペレータの身体部分が危険ゾーンに入るのを防げるように設計され、設置されている必要があります。

サブパートS (1910.399)は、OSHA電気要件について記述しています。設備または装置は、労働次官補の認可を受け、許可、認定、リスト、ラベルを受けているか、NRTL (国家承認試験研究所)によって安全性を認められている場合は、サブパートSの意義の範囲内で認可されます。

「装置」とは、電気設備の一部として、または接続して使用される素材、建具、デバイス、器具、付属品、器材などを意味します。

「リストされる」とは、その装置が、(a)当該装置の製品を定期的に調査している国家承認の研究所によって公開されているか、(b)国家承認規格を満たしている、または指定された方法で使用上の安全性が確認されたと明言されたリストに記載されているのと同等であることを意味します。

2009年8月現在、OSHAに承認されているNRTL (国家承認試験研究所)を以下に示します。

- Canadian Standards Association (CSA)
- Communication Certification Laboratory, Inc. (CCL)
- Curtis-Straus LLC (CSL)
- FM Approvals LLC (FM)
- Intertek Testing Services NA, Inc. (ITSNA)
- MET Laboratories, Inc. (MET)
- NSF International (NSF)
- National Technical Systems, Inc. (NTS)
- SGS U.S. Testing Company, Inc. (SGSUS)
- Southwest Research Institute (SWRI)
- TUV America, Inc. (TUVAM)
- TUV Product Services GmbH (TUVPSG)
- TUV Rheinland of North America, Inc. (TUV)
- Underwriters Laboratories Inc. (UL)
- Wyle Laboratories, Inc. (WL)

一部の州では独自にOSHAの支部を承認しているところもあります。24の州、プエルトリコ、およびバージン諸島では、OSHA公認の州のプランを作成し、独自の規格と実施方針を採用しています。多くの場合、これらの州では連邦OSHAと同じ規格を採用しています。しかし、一部の州ではこの項目に適用できる異なる規格または実施方針を採用しています。事業者には事故の履歴をOSHAに報告する義務があります。OSHAでは事故の発生率を累計し、その情報を支局に報告して、この情報を使用して調査の優先度を決定します。主要な検査要因は以下の通りです。

- 差し迫った危険
- 大惨事および死亡事故
- 従業員の不満
- 危険度の高い業種
- 局地的に計画された検査
- 追跡検査
- 連邦および地方の集中プログラム

OSHA規格に違反した場合は罰金が徴収されます。罰金の一覧を以下に示します。

- 重大：違反1件につき、最高7000ドル
- 重大以外：7000ドルを超えない範囲で自由裁量
- 2回目以降：違反1件につき、最高70,000ドル
- 故意：違反1件につき、最高70,000ドル
- 違反による死亡事故：追徴金
- 改善なし：1日ごと7000ドル

以下の表に、2004年10月から2005年9月までのOSHA違反上位14項目を示します。

規格	説明
1910.147	危険な動力の管理(ロックアウト/タグアウト)
1910.1200	危険有害性の周知
1910.212	すべての機械に対する一般的必要条件
1910.134	呼吸器の保護
1910.305	一般的な使用に対する配線方法、器具、設置
1910.178	産業用動力駆動運搬車
1910.219	機械的伝道装置
1910.303	一般要件
1910.213	木工機械の必要条件
19102.215	砥石車機械
19102.132	一般要件
1910.217	機械的なパワープレス
1910.095	職場での騒音への暴露
1910.023	床および壁の開口部および穴の防護

カナダの規制

カナダでは、産業安全は州レベルで管理されています。州ごとに独自の規格を維持し、施行しています。例えば、オンタリオ州では労働安全衛生法を制定し、職場のすべての当事者に権利と義務を設定しています。この法規の主な目的は、職場での労働者の健康と安全を確保することです。この法規では、職場の危険性への対処方法について詳細な手順を確立して、任意では遵守が達成されない部分への法の執行を規定しています。

この法規の規定851、第7項では、始動前の安全衛生点検を定義しています。この点検は、オンタリオ州内のあらゆる機械の新築、改築、または修正部分に対する必須事項であり、専門の技術者によるレポートの作成が要求されます。

規格

ここでは、機械安全に関する典型的な国際規格および国家規格をいくつか取り上げます。完全な表を示すのではなく、標準化の対象となる機械安全に関する問題を把握することが目的です。

「法規」の項も併せて参照してください。

世界中の国々が規格の国際的な調和に向けて努力しています。これは特に機械安全の分野で顕著に表れています。国際的な機械の安全規格は、ISOとIECの2つの機関によって管理されます。地域規格と国家規格は引き続き存在していて、地域の必要事項をサポートしていますが、ほとんどの国は、ISOおよびIECによって制定された国際規格を採用する方向に動いています。

例えば、EN (欧州標準)規格は、EEAの国々で使用されています。新しいEN規格は、すべてISOおよびIEC規格と協調していて、多くの場合、同じ文章が使用されています。

IECは電気工学的問題に対応し、ISOはその他のすべての問題に対応しています。先進工業国のほとんどがIECおよびISOのメンバーになっています。機械安全規格は、世界中の先進工業国から集められた専門家によるワーキンググループによって作成されます。

ほとんどの国では規格は任意規格として捉えることができるのに対し、法規は法的に必須です。通常、規格は法規の実用的な解釈として使用されます。したがって、規格と法規は綿密に関連し合っていると言えます。

規格のすべてのリストについては、以下のWebサイトから入手可能なセーフティカタログを参照してください: www.ab.com/safety

ISO (国際標準化機構)

ISOは、世界のほとんどの国(本書の発行時には157か国)の国家規格本体から構成される非政府機関です。スイスのジュネーブにある中央事務局が組織を統制しています。ISOでは、機械をより効果的で、安全で、手際よく設計、製造、使用するための規格を制定します。この規格により各国との貿易も容易になります。

ISOの機械規格は、EN規格と同様にタイプA、B、およびCの3段階で構成されています(「EN (欧州統一)規格」を参照)。

詳細は、ISOのWebサイトをご覧ください：*www.iso.org*

IEC (国際電気標準会議)

IECは、電気、電子、および関連技術に関する国際基準を作成し、公開しています。IECはそのメンバーを介して、電気工学的規格への適合の評価など電気工学の標準化およびその関連事項のあらゆる問題に対して国際的な協力を促進しています。

詳細は、IECのWebサイトをご覧ください：www.iec/ch

EN (欧州統一)規格

これらの規格は、すべてのECおよびEFTA加盟国に共通するもので、欧州標準化機関CENおよびCENELECによって作成されます。これらの使用は任意ですが、これに合わせて機器を設計および製造することが、EHSRへの準拠を証明するためのもっとも直接的な方法です。

これらは、3つのグループ(A、B、およびC規格)に分かれています。

タイプA規格：あらゆる種類の機械に適用できる局面をカバーします。

タイプB規格：さらに2つのグループに分割されます。

タイプB1規格：機械の特別な安全性と人間工学に関わる局面をカバーします。

タイプB2規格：安全関連部品および安全装置をカバーします。

タイプC規格：特殊なタイプまたはグループの機械をカバーします。

C規格に準拠することによって、自動的にEHSRへの適合が推測されることに注目してください。C規格に適合しない場合、AおよびB規格を使用して関連するセクションへの準拠を指摘することにより、部分的または完全にEHSRへの準拠を証明することができます。

CEN/CENELECおよびISOなどの機関間の協力に関して、他の世界中の標準化機関と合意に達しました。ここから最終的には共通の世界基準が生まれなければなりません。多くの場合、EN規格はIECまたはISOと同等です。一般的にこの2つのテキストは同じですが、規格の遵守に対して地域差があります。

EN機械安全規格の完全なリストについては、以下のWebサイトをご覧ください。

http://ec.europa.eu/enterprise/sectors/mechanical/machinery/index_ en.htm

米国の規格

OSHA規格

OSHA では、可能な限り国民的合意規格や確立された連邦規格を安全規格として推奨しています。参照文書として掲載参照することにより組み込まれている規格の必須条項(「～なければならない」という言葉は必須であることを意味する)は、パート1910に列挙されている規格と同じ効力および影響力を持ちます。例えば、国民的合意規格NFPA 70は、29 CFRのパート1910、サブパートS-電気の補遺Aに参照文書として掲載されています。NFPA 70は、全国防火協会(NFPA)によって作成された任意規格です。NFPA 70は米国電気規約(NEC)としても知られています。これにより、NECの必須条件はすべてOSHAでも必須となります。

ANSI規格

米国規格協会(ANSI)は、米国の民間部門自主標準化システムの管理者およびコーディネータとしての役割を果たしています。これは民間レベルで非営利の会員組織であり、民間部門および公共部門を通じ多様な組織の支持を受けています。

ANSIそのものは規格の策定は行ないませんが、適格と認められたグループ間での合意をとりつけることにより規格の開発を促進しています。ANSIはまた合意に達するために従うべき原則、正当な手続きや公開性がそれらのグループにより確実に守られるよう保証します。

これらの規格は、アプリケーション規格または構造規格のいずれかに分類されています。アプリケーション規格は、安全保護対策を機械に適用する方法について定義しています。ANSI B11.1ではパワープレスへの機械防護の使用方法を示す例を紹介しており、ANSI/RIA R15.06ではロボット保護のための安全保護対策の概要を説明しています。

全米防火協会

全米防火協会(NFPA)は1896年に組織されました。その使命は、火災やそれに関連する安全性の問題について科学的根拠に基いた法令や規格、研究および教育を提唱することにより、クオリティ・オブ・ライフの見地から火災の心配を低減することにありました。NFPAはこの使命の達成のために多くの規格のスポンサーとなっています。産業安全と安全保護に関係する2つの非常に重要な規格には、米国電気綱領(NEC)と産業用機械の電気規格があります。

全米防火協会は、1911年から電気綱領(NEC)のスポンサーとしての役割を果たしてきました。規格の最初の文書は1897年に、さまざまな保険、電気、建設、および関連業界の協力を得て策定されました。その後NECは度重なる改版を重ねほぼ3年ごとに改定されています。NFPA 79条では産業用機械について詳細に規定しており、産業用機械の電気規格であるNFPA 79についても触れています

NFPA 79は、公称電圧600V未満で動作する産業用機械の電気/電子装置、機器、またはシステムに適用されます。NFPA 79の目的は、産業用機械の一部として提供された電気/電子装置、機器、またはシステムの利用に関する詳細な情報を提供し、生命や財産上の安全を推進することにあります。1962年に正式に採用されたNFPA 79は国際電気標準会議規格であるIEC 60204-1の内容に非常に類似しています。

OSHA規格では特に触れられていない機械類は、死亡または重い傷害をもたらす可能性のある危険が認められないものでなければなりません。これらの機械は、該当する業界基準の必要条件に適合またはそれを超えるように設計および保守がされていなければなりません。NFPA 79はOSHA規格では特に対象とされていない機械に適用される規格です。

カナダの規格

CSA規格は、製造業者、消費者、小売業者、組合、および職能団体、政府機関を含む、生産者とユーザの国内合意を反映しています。この規格は工業および商業で広く使用されており、市役所、州政府、連邦政府でも、特に衛生、安全、ビルや建築物、および環境の分野で、条例に取り入れることもめずらしくありません。

カナダ国内の個人、企業、および団体は、CSA協会の作業にボランティアとして時間とスキルを提供したり、協会の常駐メンバーとして方針を支持することによりCSAの規格作成への指示を表しています。7000人を超える委員ボランティアと、2000人の常駐メンバーの合計がCSAの全メンバーになります

カナダ規格委員会(SCC：Standards Council of Canada)は、国家規格システム、独立連盟、自治組織が統合された団体で、国益の自主基準のさらなる作成および改善に向けて努力しています。

オーストラリアの規格

これらの規格のほとんどが、同等のISO/IEC/EN規格と足並みをそろえています。

Standards Australia Limited
286 Sussex Street, Sydney, NSW 2001
電話: +61 2 8206 6000
Eメール: mail@standards.org.au
Webサイト: www.standards.org.au

規格のコピーを購入するには、以下にご連絡ください。

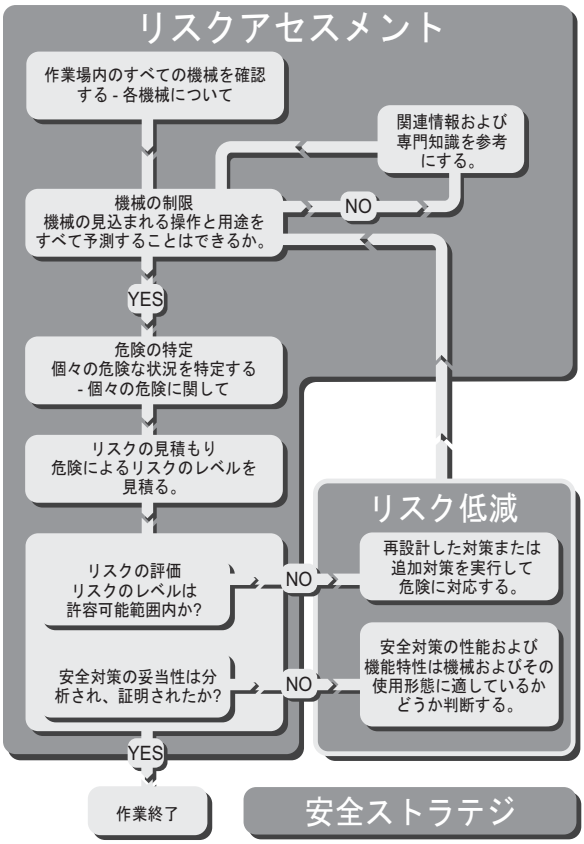
SAI Global Limited
286 Sussex Street, Sydney, NSW 2001
電話: +61 2 8206 6000
Fax: +61 2 8206 6001
Eメール: mail@sai-global.com
Webサイト: www.saiglobal.com/shop

規格のすべてのリストについては、以下のWebサイトから入手可能なセーフティカタログを参照してください: www.ab.com/safety

安全ストラテジ

純粋に機能の観点からみると、機械は材料を処理する作業をより効果的に実行できればそれだけ優れていることになります。しかし、機械が機能し続けるためには、同時に安全でなければなりません。

適切な安全ストラテジを考案するには、下図に示すように以下のことが必要です。



リスクアセスメントは、機械の制限、機能、および作業を明確に理解することに基づいており、全寿命を通じて機械で実施する必要があります。

リスク低減は、必要に応じて実行され、安全対策は、リスクアセスメントの段階で引き出された情報に基づいて選択されます。これを実施する方法が、安全ストラテジの基礎になります。

そのためには、すべての局面が考慮されているか、原則を無視することで詳細を見失っていないか確認するための参考になるチェックリストが必要です。すべてのプロセスが文書化されているか確認します。これでさらに充実した作業が約束されるだけでなく、他の関係者がその結果を使用してチェックできるようになります。

このセクションは、機械製造メーカと機械ユーザに適用されます。機械製造メーカは、マシンを安全に使用できることを求めています。リスクアセスメントはマシン設計段階から始めて、マシンで実行する必要がある予測可能なタスクをすべて考慮する必要があります。リスクアセスメントの早期の反復というアプローチに基づくこの作業が非常に重要です。例えば、マシンの可動部品を定期的に調整する必要がある場合に、測定で設計するのが可能設計段階ではこのプロセスを安全に行なうことができます。初期段階で見過ごすと、最後の段階では実装は困難であるかまたは不可能であることがあります。その結果、可動部品の調整を行なう必要がありますが、非安全または効率の悪い(または両方)手段で実行することになります。すべてのタスクでリスクアセスメントを行なったマシンは、より安全で効率的なマシンになります。

ユーザ(または事業者)は、安全な作業環境を備える必要があります。マシンが安全であると機械製造メーカによって断言されていたとしても、マシンユーザが機器が安全な環境にあるかを判断するためにリスクアセスメントを実行する必要があります。マシンは、機械製造メーカによって予期しない状況で使用されることが多くあります。例えば、学校の作業室で使用されるフライス盤には、工場の工具室で使用されるとき以上の考慮が必要になります。

さらに、企業ユーザが2つ以上の独立した機械を所有していて、それらを1つのプロセスに統合する場合、技術的に言えば、ユーザは結合した結果として出来上がった機械の製造メーカになることも忘れてはなりません。

そこで、適切な安全ストラテジにたどり着く途中の重要なステップについて考えます。以下の対策は、すでに工場に設置されている機械にも、新しい単体の機械にも適用できます。

リスクアセスメント

リスクアセスメントを負担と見なすのは間違っています。これはユーザや設計者が安全を達成する方法に関する論理的な決定を取るのに極めて重要な情報を提供して、権限を与えるのに役立つ過程です。

さまざまな規格でこのテーマについて記載されています。ISO 14121: 「リスクアセスメントの原則」およびISO12100:「機械安全−基本原則」には、ほぼ世界中で適用できるガイダンスが記載されています。

リスクアセスメントを行なうのに使用するテクニックとして、通常、さまざまな人が参加している機能的なチームで行なうほうが、個人で行なうよりもより広い適用範囲とバランスでより良い結果を生みます。

リスクアセスメントは反復プロセスで、マシンのライフサイクルのさまざまなステージで実行できます。使用可能な情報は、ライフサイクルのステージごとで異なります。例えばマシンビルダーで実施されるリスクアセスメントでは、詳細なマシンのメカニズムと構造の材質にアクセスしますが、おそらくは、マシンの根本的な作業環境はおおよその仮定でしかありません。機械ユーザで実施されるリスクアセスメントは、技術的な詳細に掘り下げてアクセスする必要はありませんが、マシンの作業環境の詳細にはアクセスします。理想では、1つの反復の出力は、次の反復の入力になります。

機械の制限の特定

情報を集めて分析することが必要です。また、マシンに対して人が行なう作業内容をすべてと、マシンを稼動する環境考慮する必要もあります。マシンとその使用の明確に理解するために目的物を取得します。

機械的にまたは制御システムによってかのいずれかで個別のマシンが互いにリンクされている場合、適切な保護手段で「ゾーン化」されるまで1台のマシンとして考慮する必要があります。

危険の特定の段階と同様、導入時、稼働時、メンテナンス時、廃棄時など、機械を使用している間のあらゆる段階について、正しい使用法および操作だけでなく、当然予測できる誤用または故障の影響も考慮することが重要です。

タスクおよび危険の特定

マシンに存在する危険のすべてを、特性と場所の観点から特定してリストする必要があります。あらゆるタイプの危険を考慮する必要があります。例えば、押しつぶし、切断、引込み、部分噴出、蒸気、放射線、有害物質、熱、騒音などがあります。

タスク分析の結果を、危険の特定の結果と比較する必要があります。これは、危険や人の集中する場所、つまり危険な状況になる可能性があること示します。危険な状況のすべてをリストする必要があります。同じ危険であっても、人やタスクの特性によっては異なるタイプの危険な状況を生み出すことになります。例えば、非常に高いスキルとトレーニングを受けた保守要員が存在する場合と、マシンに対する知識のない未熟な掃除人とでは影響が異なります。この状況では、それぞれのケースを個別にリストして特定するときに、掃除人のそれとくらべて保守要員の保護方式が異なることを証明する必要があることがあります。ケースが別々にリストされていて特定されていない場合は、最悪の場合は使用すべきで、保守要員と掃除人は同じ保護方式で共にカバーできます。

場合によっては、既に保護対策が行なわれている既存のマシン(例えば、危険な可動部が連動している防護ドアによって保護されているマシン)上でも、一般的なリスクアセスメントを行なう必要があります。危険な可動部は、連動するシステムが故障した場合に実際の危険になるかもしれない潜在的な危険です。まだそのインターロックシステムを有効にしていない場合は(例えば、適切な規格へのリスクアセスメントによるかまたは設計による)、その存在を考慮に入れるべきではありません。

リスクの見積もり

これは、リスクアセスメントの最も基本的な側面です。この対象に取り組むには多くの方法があり、以下のページに基本原理を示します。

危険な状況の可能性を持っているマシンには、すべて危険なイベント(すなわち、害)の危険が存在します。危険が大きければ大きいほど、それに対する処置がより重要になります。ある危険ではリスクが非常に低いため許容できますが、別の危険ではリスクが非常に大きいために、保護手段として大きな措置をとる必要がある場合があります。そのため、「リスクに関してするべきこと」を決定するために、それを定量化する必要があります。

リスクという言葉は、事故の深刻さと混同されることがよくあります。潜在的な被害の深刻さと発生の確率の両方を考慮して、存在するリスクの量を見積もります。

このページに示すリスクの見積もりの提案は、異なる基準法で決めているため、個別の事情には使用しないでください。これについては、整然としてドキュメント化された構造を奨励するために、一般的ガイドラインとしてのみ示しています。

使用するポイントシステムはどんな特定のタイプの適用のためにもキャリブレーションされていないため、それがアプリケーションに適していない場合があります。ISO TR (テクニカルレポート) 14121-2 “Risk assessment‐Practical guidance and examples of methods”は、実際的なガイダンスを提供し、リスクを定量化するさまざまな方法を示します。

以下の要因について考慮してください。

- 潜在的な傷害の重大度
- それが発生する確率

発生の確率には、次の2つの要素が含まれます。

- 発生の頻度
- 傷害の可能性

各要因を個別に取り扱うことで、これらの要素に評価を与えます。

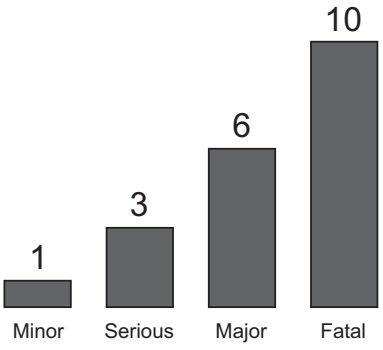
可能な限りあらゆるデータと経験を利用します。機械寿命のすべての段階に対応することになるので、最悪のケースに基づいて決定します。

また、常識を保有するのも重要です。決定は、可能で、現実的でもっともらしいことを考慮に入れる必要があります。これは、交差している機能的なチームアプローチが貴重であるところです。

忘れてならないのは、これを実行する上で、保護システムはまだ適応されていない、または危険性がないことを前提としなければならないことです。このリスク見積りが保護システムが必要であることを示す場合は、必要な特性を決定するための方法論がいくつかあり、それについてはこのセクションの後で説明します。

1. 潜在的な障害の重大度

この点について検討するために、下図に示すような危険の結果として事故または事件が発生したと想定します。危険性について注意深く調査すると、考えられる最も深刻な障害は何かが明らかになります。注意：これを検討するにあたり、傷害は避けられないと想定し、その重大度のみに注目しています。オペレータが危険な動作またはプロセスにさらされていると想定しています。傷害の重大度は、以下のように評価されます。



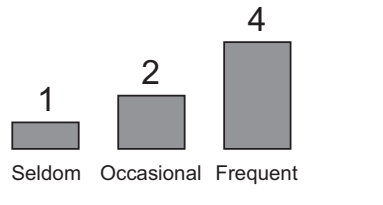
傷害の重大度が割付けられたポイント

- **FATAL** (致命的)：死亡
- **MAJOR** (重大：通常は不可逆的)：永久的な能力喪失状態、失明、四肢切断、呼吸器障害など
- **SERIOUS** (重傷：通常は可逆的)：意識消失、火傷、骨折
- **MINOR** (軽傷)：打撲、切り傷、すり傷など

各説明は、左図に示すようにポイント値に割付けられています。

2. 発生の頻度

発生の頻度とは、オペレータまたは保守要員がどれくらいの頻度で危険にさらされるかです。危険発生の頻度は、以下のように分類されます。



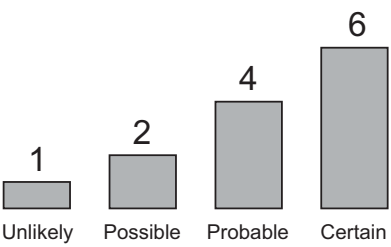
発生の頻度が割付けられたポイント

- **FREQUENT** (頻繁)：1日の数回
- **OCCASIONAL** (時折)：毎日
- **SELDOM** (まれ)：週1回以下

各説明は、左図に示すようにポイント値に割付けられています。

3. 障害の可能性

オペレータが危険な動作またはプロセスにさらされていると想定しています。オペレータが機械およびその他の要素(始動時の速度、など)によってどのような影響を受けるかを考えることにより、傷害の可能性を、以下のように分類することができます。



傷害の可能性が割付けられたポイント

- **UNLIKELY** (あり得ない)
- **PROBABLE** (可能性大)
- **POSSIBLE** (可能性有り)
- **CERTAIN** (確実)

各説明は、左図に示すようにポイント値に割付けられています。

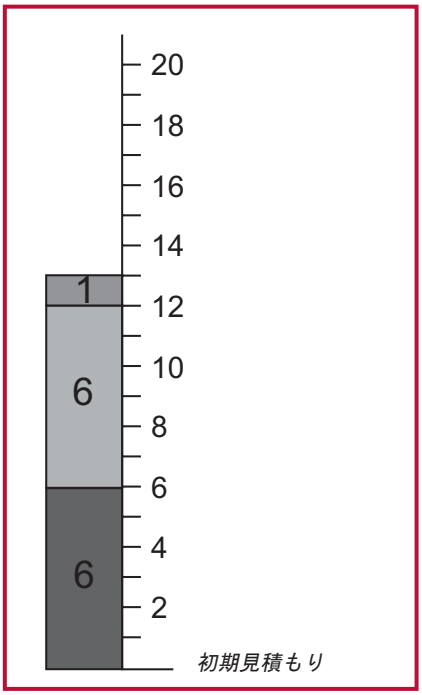
上部の数字は割付けられている値で、これらを加算することで、初期見積りが得られます。最大13の値までの3つのコンポーネントの加算を示しますが、以下に示す他の要素も考慮することによって、初期見積りを調整する必要があります(注：これは、前述の図の例に基づくものではありません)。

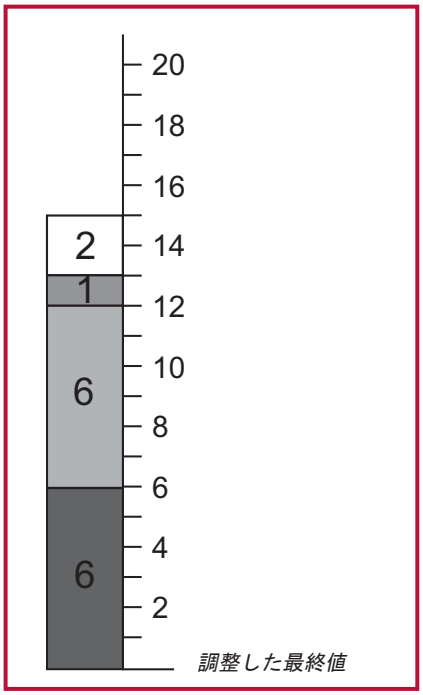
次のステップでは、以下の表に示す他の要素も考慮することによって、初期見積りを調整します。正しく検討できるのは、通常、機械が永続的な場所に設置されている場合だけです。

典型的な要素	処置
複数の人間が危険にさらされる。	重大度の要素に人数を掛ける。
危険領域で電源が完全に遮断されない状態が長く続く。	1回の接近にかかる時間が15分を超える場合、頻度要素に1ポイント加算する。
オペレータが技術者でないか、トレーニングを受けていない。	合計に2ポイント加算する。
接近の間隔が非常に長い(例えば1年)。(特にモニタシステムに、進行性および未発見の故障がある可能性がある。)	最大頻度要素と同等のポイントを加算する。

リスク見積もりに関する追加の注意事項

追加要素を考慮した結果は、以下に示すように前述の合計に加算されます。





リスク低減

次に、個々の機械とそれに関するリスクを順番に検討し、すべての危険に対する対策を講じます。

以下に示すチャートは、使用している機械の安全性をあらゆる局面から明らかにする、文書化されたプロセスの一部を表しています。これは、機械ユーザのガイドとして使用できますが、機械メーカまたはサプライヤも、同じ原理を使用して、すべての機器が評価されているか確認することができ、リスクアセスメントについてより詳細にレポートするためのインデックスとしても使用されます。

この図から、機械にCEマークが付けられている場合、機械の危険性が機械メーカによってすでに評価されているので、処理が簡単になることと、必要な手段がすでに取られていることがわかります。CEマークが付けられた装置であっても、機械メーカでは予測できない用途の性質や処理される材料による危険は、まだ存在している可能性があります。

Company - MAYKIT WRIGHT LTD
Facility - Tool room - East Factory.
Date - 8/29/95
Operator profile - skilled.

Equipment Identity & Date	Directive Conformity	Risk Assessment Report Number	Accident History	Notes	Hazard Identity	Hazard Type	Action Required	Implemented and Inspected - Reference
Bloggs center lathe. Serial no. 8390726 Installed 1978	None claimed	RA302	None	Electrical equipment complies with BS EN 60204 E-Stops fitted (replaced 1989)	Chuck rotation with guard open	Mechanical Entanglement Cutting	Fit guard interlock switch	11/25/94 J Kershaw Report no 9567
					Cutting fluid	Toxic	Change to non toxic type	11/30/94 J Kershaw Report no 9714
					Swarf cleaning	Cutting	Supply gloves	11/30/94 J Kershaw Report no 9715
Bloggs turret head milling m/c Serial no 17304294 Manuf 1995 Installed May 95	M/c Dir. EMC Dir	RA416	None		Movement of bed (towards wall)	Crushing	Move machine to give enough clearance	4/13/95 J Kershaw Report no 10064

リスク低減手段のヒエラルキー

以下の3つの基本的な手段を、記述されている順番に考慮して使用するように説明しています。

1. できる限りリスクを排除または低減します(本質的に安全な機械の設計および構造)。
2. 排除できないリスクに対して必要な保護手段(例：インターロック付きガード、ライトカーテンなど)を講じます。
3. 採用された保護手段が不十分なために未解決のリスクについて、ユーザに通知し、特別なトレーニングが必要かどうかを示し、さらに個人用保護具を用意する必要があれば指定します。

ヒエラルキーの各手段は、上から順番に考慮して可能であれば使用する必要があります。通常、これらの手段を組み合わせて使用します。

本質的に安全な設計

機械設計の段階で、材質、アクセス要件、熱面、通信方法、トラップポイント、電圧レベルなどの要因を注意して考慮することによって多くの危険の可能性をできるだけ簡単に防ぎます。

例えば、危険領域に近づく必要がない場合、保護対策は、マシンのボディ内での安全ガードまたは固定式保護ガードのいずれかのタイプになります。

保護システムおよび手段

接近する必要がある場合は、状況は多少困難になります。機械が安全なときだけ、接近できるようにする方法を確保することが必要です。インターロック付き防護ドアやトリップシステムなどの保護手段が必要になります。保護装置または保護システムの選択は、機械の操作特性に強い影響を受けます。機械の効率を損なうシステムは、権限なしで排除されたり、無視されたりする傾向があります。

この場合の機械の安全性は、フォルト状態でも、保護システムを適切に適用し、正しく操作できるかどうかに左右されます。これで、アプリケーションは適切な保護システムによって対応されたことになります。

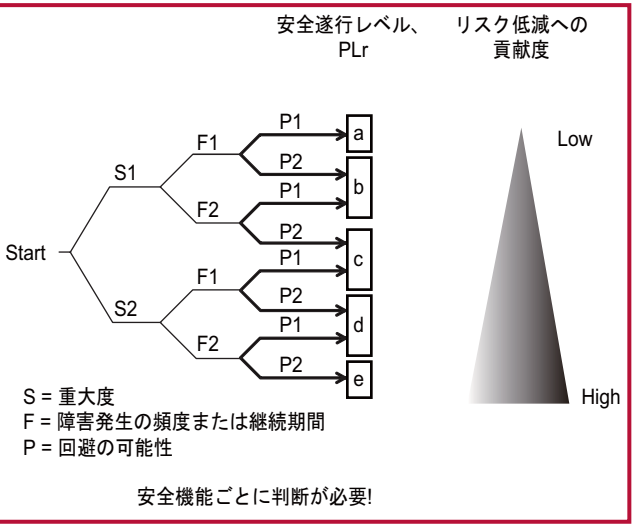
今度はシステムの正しい操作について考慮する必要があります。それぞれのタイプには、さまざまなレベルのフォルトモニタ、検出、または阻止能力を備えたテクノロジの選択肢があります。

理想を言えば、どの保護システムも、危険な状況に陥る可能性が完全になくなれば完璧です。しかし、現実には、現在の知識および資料の限界によって制約されています。もう1つの非常に現実的な制限はもちろんコストです。これらの要素から、平衡感覚が必要であることが明らかになります。常識で考えれば、ワーストケースでも軽い打撲を与える可能性のある機械の安全システムの整合性は、ジャンボジェットを飛ばすために必要とされるのと同じだと言い張るのは、ばかげています。故障の影響は大幅に異なるので、保護手段が及ぶ範囲と、リスク見積りの段階で判明した受けるリスクのレベルとを関係付ける方法をいくつか用意する必要があります。

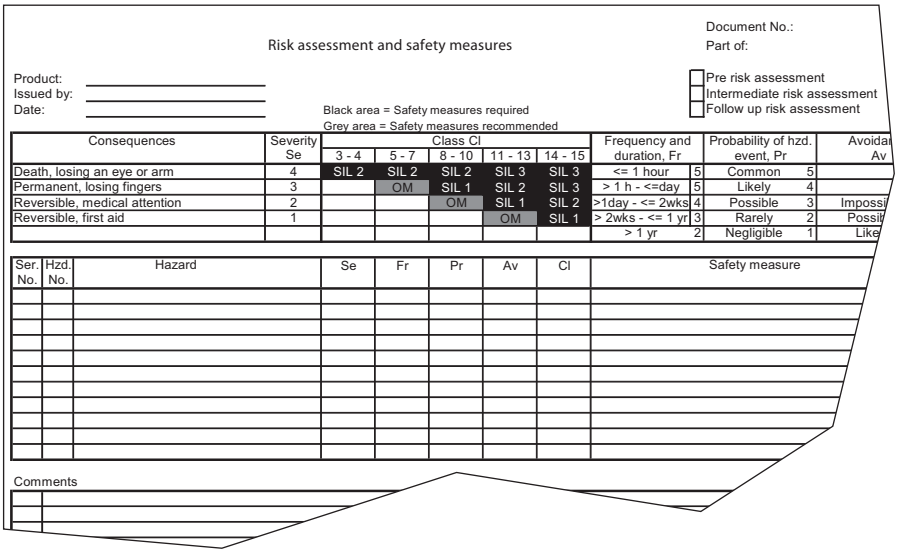
どのタイプの保護装置を選択するとしても、「安全関連システム」には保護装置、配線、電源スイッチ装置、ときには機械の運転管理システムの一部などを始めとして多くの要素が含まれることを忘れることはできません。システムのこれらの要素(ガードの組込み、取付け、配線など)はすべて、それぞれの設計原理やテクノロジに適したパフォーマンス特性を備えている必要があります。IEC/EN 62061およびEN ISO13849-1は、システム制御の安全関連部分のパフォーマンスの階層的なレベルを分類しており、その付録に保護システムの整合性要件を判断するためリスクアセスメント手段を記載しています。

EN ISO 13849-1:2008は、付録Aに高度なリスクグラフを記載しています。

マシンの安全関連制御システム



IEC 62061でも、付録Aに以下に示すような形式で方法を説明しています。



Risk assessment and safety measures

Document No.:
Part of:

Product:
Issued by:
Date:

☐ Pre risk assessment
☐ Intermediate risk assessment
☐ Follow up risk assessment

Black area = Safety measures required
Grey area = Safety measures recommended

Consequences	Severity Se	Class Cl 3 - 4	5 - 7	8 - 10	11 - 13	14 - 15	Frequency and duration, Fr		Probability of hzd. event, Pr		Avoida Av
Death, losing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1 hour	5	Common	5	
Permanent, losing fingers	3		OM	SIL 1	SIL 2	SIL 3	> 1 h - <=day	5	Likely	4	
Reversible, medical attention	2			OM	SIL 1	SIL 2	>1day - <= 2wks	4	Possible	3	Impossi
Reversible, first aid	1				OM	SIL 1	> 2wks - <= 1 yr	3	Rarely	2	Possi
							> 1 yr	2	Negligible	1	Like

Ser. No.	Hzd. No.	Hazard	Se	Fr	Pr	Av	Cl	Safety measure

Comments

上記の方法のどちらを使用しても、同じ結果が得られます。どちらの方法も、関連する規格の詳細な内容を考慮できるようになっています。

どちらの場合も、規格の本文に記載されているガイダンスが使用されていることが極めて重要です。リスクのグラフまたは表は、単独で、または過度に単純化した方法では使用しないでください。

評価

防護手段を選択したら、導入する前にリスクの見積りを繰返し行なうことが重要です。この手順は見過ごしがちです。防護手段を設置すると、マシンオペレータは本来予想されるすべてのリスクから完全に保護されていると感じることがあります。オペレータは危険に対する本来の認識を失うため、機械に介入する方法を変える可能性があります。例えば、危険に曝される機会が増えたり、機械に近寄りすぎる危険性があります。これは、保護手段が機能しない場合、以前に予想されていたよりも大きなリスクにさらされることを意味します。これが見積りが必要な堅実的リスクです。したがって、リスクの見積りは、オペレータの機械への介入方法に関して予測できる変化をすべて考慮した上で、繰返し行なう必要があります。この作業の結果を使用して、提案された保護手段が実際に適しているかチェックします。詳細は、IEC/EN 62061の付録Aを参照してください。

トレーニング、人体用保護具など

オペレータは、機械の安全な作業方法について必要なトレーニングを受けていることが重要です。それで他の手段を省略できるわけではありません。オペレータに危険領域には近づかないように指示するだけでは(保護対策のかわりとしては)不十分です。

オペレータが特殊なグローブ、ゴーグル、呼吸マスクなどの防具を使用しなければならないこともあります。機械設計者は、必要な防具の種類を指定する必要があります。個人用保護具の使用は、一般的に主要な防護手段にはなりませんが、前述の手段を補完することになります。

規格

多くの規格とテクニカルレポートでは、リスクアセスメントに関するガイダンスを示しています。中には広範囲に適用できるものもあれば、特定のアプリケーションを対象に書かれているものもあります。以下に、リスクアセスメントに関する情報が含まれている規格の一覧を示します。

ANSI B11.TR3：リスクアセスメントおよびリスク低減 – 機械装置に関するリスク見積、評価、低減のガイド

ANSI PMMI B155.1：梱包マシンおよび梱包関連の加工機械に関する安全要件

ANSI RIA R15.06：産業用ロボットおよびロボットシステムの安全要件

AS 4024.1301-2006：リスクアセスメントの原則

CSA Z432-04：機械の安全保護対策

CSA Z434-03：産業用ロボットおよびロボットシステム – 一般的な安全要件

IEC/EN 61508：電気、電子、およびプログラマブル電子安全関連システムの機能安全

IEC/EN 62061：機械安全 – 安全関連の電気、電子、およびプログラマブル電子制御システムの機能安全

EN ISO 13849-1：機械安全 – 制御システムの安全関連部分

EN ISO 14121-1： リスクアセスメントの原則

ISO TR 14121-2：リスクアセスメント – 手段の実際的なガイダンスおよび例

保護手段および補助的な装置

リスクアセスメントによって、機械またはプロセスが傷害のリスクを伴うことが示された場合、その危険は排除または抑制する必要があります。これを実現する方法は、機械と危険の性質によって決まります。ガードと共に使用する保護手段は、危険への接近を阻止するまたは危険への接近を検出する手段として定義されます。標準的な保護手段には、インターロック付きのガード、ライトカーテン、セーフティマット、両手用制御、およびイネーブルスイッチがあります。

非常停止装置およびシステムは安全関連制御システムに関連していますが、直接的な保護システムではなく、補助的な保護手段としてのみみなす必要があります。

固定式保護ガードによる接近の阻止

危険箇所が、接触する必要のない機械の一部である場合は、固定式保護ガードで永久的にガードすることが望まれます。このタイプのガードを取り外すには、工具が必要です。固定式保護ガードには、1) 動作環境に耐えられること、2) 必要に応じてプロジェクタイルを組み込む、3) それ自体が鋭利な角などによって危険を誘発しないことが要求されます。固定式保護ガードには、ガードが機械に接する場所に開口部がある場合や、エンクロージャをワイヤ・メッシュ・タイプにすることで開口部をつくる場合もあります。

窓があると、そこから機械にアクセスして機械の動作をモニタしやすくなります。切削液との化学的相互作用、紫外線、および単純に老朽化により窓の素材が次第に劣化するため、使用する材質は十分注意して選択する必要があります。

開口部の大きさは、オペレータが危険箇所に接触できないサイズでなければなりません。米国のOHSA 1910.217 (f) (4)の表O-10、ISO 13854、ANSI B11.19の表D-1、CSA Z432の表3、およびAS4024.1に、特定の開口部と危険箇所との適切な距離に関する指針が示されています。

接近の検出

保護手段は、危険箇所へのアクセスを検出するために使用されます。リスク低減の方法として検知が選択された場合、設計者は完全な安全システムを使用する必要があること、安全保護装置だけでは十分にリスクを低減できないことを理解している必要があります。

この安全システムは、通常、以下の3つのブロックで構成されます。

1) 危険箇所へのアクセスを感知する入力装置
2) 検知装置からの信号を処理し、安全システムの状態をチェックして、出力装置をオンまたはオフにするロジックデバイス
3) アクチュエータ(モータなど)を制御する出力装置

検出装置

危険領域に入ろうとする人や、危険領域内にいる人を検知するには、さまざまな種類の装置を使用できます。特定の用途に最適な装置は、次の要素を考慮して選択します。

- アクセスの頻度
- 危険部分の停止時間
- マシンサイクルを完了させることの重要性
- プロジェクタイル、液体、霧、蒸気、などの遮蔽

適切に選択された可動式ガードは、インターロックすることでプロジェクタイル、液体、霧、および他のタイプの危険から保護することができ、危険箇所にほとんどアクセスしない場合によく使用されます。マシンサイクルの間や、機械が停止するまでに時間がかかる場合にはインターロックガードをロックすることで、アクセスできないようにすることもできます。

ライトカーテン、マット、およびスキャナなどの存在検知装置は、危険領域に素早く簡単にアクセスできるため、オペレータが危険領域に頻繁にアクセスする必要がある場合に選択されます。このタイプの装置は、プロジェクタイル、霧、液体、その他のタイプの危険物を防ぐことはできません。

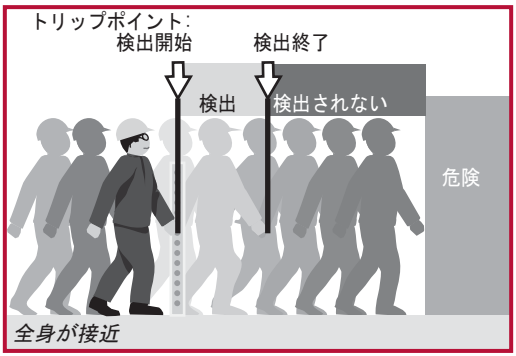
通常の機械動作の妨害を最小限に抑えて、最大の保護を実現できる装置またはシステムが、最適な保護手段になります。実際には使いにくいシステムは、排除されたり、回避されることが多いため、機械の使用方法をあらゆる観点から検討する必要があります。

存在検知装置

領域またはエリアを保護するのを決定する際には、具体的にどのような安全機能が必要なのかを明確に把握することが重要です。一般的には、少なくとも2つの要素があります。

- 危険領域内に人が入ったら、電源のスイッチを切る、または無効にする。
- 危険領域内に人がいる間は、電源のスイッチを入れたり、有効にしたりできないようにする。

1点目を達成するには、ある種のトリップ装置を使用する必要があります。言い換えると、人体の一部があるポイントを超えたことを検出し、電源を切るための信号を発する装置です。さらに、人がトリップポイントを過ぎてもそのまま進むことができ、その存在がもはや検出されなくなった場合、2点目(スイッチが入るのを回避する)を実現できないかもしれません。



上の左図に、全身が接近する場合のこのような特性を持つ装置の例としてトリップデバイスとして垂直に取付けられたライトカーテンの例を示します。インターロック付き防護ドアも、中に入った後、ドアが閉まるのを回避する手段がないため、通常はトリップするだけの装置と見なされます。

全身が接近する可能性はないので、トリップポイントを超えて進むことができない場合は、その存在は常に検出されており、2点目(スイッチが入るのを回避する)は実現されています。

体の一部が接近するタイプのアプリケーションでは、右図に示すように同じタイプの装置がトリップ機能と存在感知機能を実行します。唯一の違いは使用形態です。

存在検知装置は、人の存在を検知するために使用されます。このタイプの装置としては、セーフティ・ライト・カーテン、シングル・ビーム・セーフティ・バリア、セーフティ・エリア・スキャナ、セーフティマット、およびセーフティエッジなどがあります。

セーフティ・ライト・カーテン

セーフティ・ライト・カーテンは、簡単にいえば光電センサであり、特に危険な機械動作から工場作業者を守るために設計されています。AOPD (アクティブ光電保護装置)またはESPE (電子感応式保護装置)としても知られているライトカーテンは最大の安全性を保証しつつ、生産性の向上にも貢献し、かつ人間工学的な見地からみて機構的な保護装置よりも安全な設備です。作業者が頻繁に、また容易に作業上危険な箇所にアクセスしなければならない場合には、ライトカーテンは高い利便性を持っています。

ライトカーテンは、IEC 61496-1および-2を満たすように設計されテストされています。パート2の整合ENバージョンはないため、欧州機械指令(European Machinery Directive)の付録IVでは、ライトカーテンをEC (欧州共同体)の市場に出す前に第三者認証を得ることを義務付けています。第三者が、この国際規格にライトカーテンが適合しているかどうかテストします。Underwriter's Laboratoryでは、IEC 61496-1を米国の国家規格として認めています。

セーフティ・レーザ・スキャナ

セーフティ・レーザ・スキャナは、回転する鏡で光パルスを円弧状に反射させて検知面を作成します。対象物の場所は、鏡の回転角から特定されます。不可視光線の反射ビームによる「飛行時間」法を使用して、スキャナから対象物までの距離も測定できます。測定された距離と対象物の場所を使用して、レーザスキャナは対象物の正確な位置を特定します。

感圧式セーフティマット

これらのデバイスは、マシン周辺のフロアをガードするために使用されます。相互接続されたマットのマトリックスは危険な領域の周辺に並べられ、マットに圧力がかかると(例：オペレータが踏む)、マット・コントローラ・ユニットが危険に対して電源をオフします。感圧式マットは、例えばフレキシブルな製造またはロボットセルなどの複数のマシンを含む囲まれた領域でよく使用されます。アセルへのアクセスが必要な(例えば、設定またはロボットのティーチのため)場合に、オペレータが安全領域からそれるか、装置の一部の背後に回らなければならないときに、危険な動きを防止します。

マットのサイズと配置を決定するには、安全距離を考慮する必要があります。

存在検知エッジ

これらのデバイスはフレキシブルなエッジストライプで、ぶつかったりはさまれたりする危険にさらされているマシンテーブルや電動ドアなどの可動部品の端に取付けることができます。

可動部品がオペレータにぶつかると(または逆)、屈曲感知式エッジが押し下げられ、危険な電源をオフするようにコマンドが起動されます。また、感知式エッジは、オペレータのリスクが絡み合う場所のマシンをガードするためにも使用されます。オペレータがマシンにはさまれたときに、感知式エッジに触れるとマシンの電源がダウンします。

セーフティエッジは、多数の技術を使用して作られています。一般的な技術の1つが、実質的には長いスイッチをエッジ内部に挿入する方法です。この方法ではストレートエッジを採用し、通常、4線式の接続方法が使用されます。

ライトカーテン、スキャナ、フロアマット、および感圧式エッジは、「トリップ装置」に分類されます。これらの装置は、実際にアクセスを阻止するのではなく、それを「感知」するだけです。これで提供できる安全性は、感知とスイッチの両方の能力に完全に依存しています。一般的に、トリップ装置を適用できるのは、電源が遮断されるとすぐに停止する機械だけです。オペレータは、危険領域に直接踏み込んだり、触れたりできるので、動作が停止するのにかかる時間が、装置をトリップしてからオペレータが危険箇所に到達するまでの時間より短くなければならないのは明らかです。

セーフティスイッチ

機械にアクセスする頻度が低い場合は、可動式(開閉可能な)保護ガードが適しています。保護ガードは、防護ドアが閉じていないときは、危険な電源が確実に遮断されるように、危険箇所の電源とインターロックされています。この方法には、防護ドアに取付けられたインターロックスイッチを使用します。危険箇所の電源の制御は、この装置のスイッチ部分を通して行ないます。電源は、通常は電気ですが、空気圧または水圧の場合もあります。防護ドアの動作(開く)を検出すると、インターロックスイッチは危険な電源の供給を直接、または電源コンタクタ(またはバルブ)を介して遮断します。

インターロックスイッチの中には、防護ドアを閉じた状態にロックし、機械が安全な状態になるまで解除しないロック装置が組み込まれているものもあります。大部分の用途では、可動式保護ガードと、ガードロック機能有りまたはなしのインターロックスイッチの組合せが最も信頼性が高く、費用効果的なソリューションといえます。

以下を含めて幅広いセーフティスイッチのオプションがあります。

- **タング式インターロックスイッチ**：これらのデバイスには、スイッチに挿入されたり、引き抜かれたりするタング型のアクチュエータが必要です。
- **ヒンジ型インターロックスイッチ**：これらのデバイスは防護ドアのヒンジピン上に配置し、ガードが開くことで作動します。
- **ガードロック機能付きスイッチ**：一部のアプリケーションでは、ガードを閉じた状態でロックするか、またはガードが開くのを遅らせることが要求されます。この要件に適した装置は、ガードロック機能付きインターロックスイッチと呼ばれるものです。これらの装置は、停止する特性を持つ機械に適していますが、ほとんどのタイプの機械で保護レベルを大幅に向上させることができます。
- **非接触型インターロックスイッチ**：これらのデバイスの不正侵入防止を高めるためにコーディング機能を組み込んだバージョンでは、作動するために物理的な接触は不要です。
- **位置(リミットスイッチ)インターロック**：カム作動式は、通常ポジティブ・モード・リミット(または位置)スイッチとリニアカムまたはロータリカムで構成されます。これらは、通常スライディングガードで使用されます。
- **トラップ・キー・インターロック**：トラップキーは、電源インターロックの他に制御インターロックを実行できます。「制御インターロック」では、インターロック装置がが中間装置に停止コマンドを指令し、それによって次の装置がオフになり、アクチュエータからエネルギーを切り離します。「電源インターロック」では、停止コマンドがマシンアクチュエータへのエネルギー供給を直接遮断します。

オペレータインターフェイス装置

停止機能：米国、カナダ、欧州、および国際的なレベルで、機械または製造システムにおける停止カテゴリの記述について合意がなされています。

注：これらのカテゴリは、EN 954-1 (ISO 13849-1)のカテゴリと異なります。詳細は、規格NFPA79とIEC/EN60204-1を参照してください。停止は、以下の3つのカテゴリに分けられます。

カテゴリ0は、機械のアクチュエータ(作動装置)への電力を即座に取り除くことで停止します。これは、無制御停止と考えられます。電源が遮断されると、電源が必要なブレーキング作用は無効になります。これによって、モータは空回りするようになり、自然に停止するまで長時間かかります。別の例では、材料を保持するために電源が必要な機械の保持固定具の場合、材料が落ちる可能性があります。電源を必要としない、機械的な停止の意味は、カテゴリ0停止と合わせて使用されることもあります。カテゴリ0停止は、カテゴリ1またはカテゴリ2停止より優先されます。

カテゴリ1は、停止させるために機械のアクチュエータで電源を使用できるようにする、制御された停止です。その後、機械が停止した時点で、アクチュエータから電力が取り除かれます。この停止カテゴリは、電動ブレーキを使用して危険な動作を迅速に止めることができ、その後でアクチュエータから電力を取り除くことができます。

カテゴリ2は、機械のアクチュエータで電源を使用可能にした状態での、制御停止です。通常の製造停止は、カテゴリ2停止と考えられます。

これらの停止カテゴリは、個々の停止機能に適用する必要があります。制御システムの安全関連部分が入力に応答して実行する停止機能の場合、カテゴリ0または1を使用する必要があります。停止機能は、対応する始動機能を無効にしなければなりません。各停止機能に合わせて停止カテゴリを選択するには、リスクアセスメントによって判断する必要があります。

非常停止機能

非常停止機能は、リスクアセスメントによる判断では、カテゴリ0またはカテゴリ1のいずれかの停止として動作する必要があります。人の1つの動作でこの機能を開始できなければなりません。さらに、起動されたら、他のすべての機能および機械の動作モードを無効にする必要があります。目的は、さらに他の危険を引き起こすことなく、できるだけ迅速に電力を取り除くことです。

最近までは、非常停止カテゴリの回路には、ハード配線で接続された電気機械部品が必要でした。IEC 60204-1およびNFPA 79などの規格の最近の変更は、IEC61508のような規格に関する要件を満たすそのセーフティPLCと他の形式の電子ロジックを意味して、非常停止回路で使用できます。

非常停止装置

オペレータが機械に関するトラブルに巻き込まれる危険性がある場合は、必ず非常停止装置に迅速にアクセスするための設備が必要になります。非常停止装置は、連続して操作することができ、常に使用可能でなければなりません。各オペレータパネルに少なくとも1つの非常停止装置が装備されている必要があります。必要に応じて、別の場所に追加の非常停止装置を使用することもできます。非常停止装置には、さまざまな形式があります。押しボタンスイッチとロープ型(ケーブルプル)スイッチが、最も一般的なタイプの装置です。非常停止装置は、作動された時点でラッチしなければならず、ラッチできなかった場合は、停止コマンドを発行できなくなることが要求されます。非常停止装置のリセットによって危険な状態を引き起こすことは許されません。別の意図的な処置を使用して、機械を再起動するようにします。

非常停止装置の詳細は、ISO/EN13850、IEC 60947-5-5、NFPA79、およびIEC60204-1、AS4024.1、Z432-94を参照してください。

非常停止ボタン

非常停止装置は、無料な安全保護設備と考えられています。これらは、危険箇所へのアクセスを防いだり、検知したりするわけではないので、主要な安全保護装置とは見なされていません。

この装置でよく使用されるのは、黄色の台に赤のマッシュルーム型押しボタンが取付けられているタイプで、オペレータは非常時にこれを押します。この装置は、危険箇所の手の届く場所に必ず1つはあるように、十分な数を機械の回りに効果的に配置する必要があります。

非常停止ボタンは、いつでも使用できる状態になっていて、機械がどの動作モードであっても使用できなければなりません。非常停止装置として押しボタンが使用されるときは、台が黄色でボタンは赤色のマッシュルーム(パームボタン)型でなければなりません。ボタンが押されると接点の状態が変化し、それと同時にボタンが押下された位置にラッチされなければなりません。

非常停止に採用されている最新の技術の1つが自己モニタ機能です。非常停止の背面に、パネル構成部品の後にまだ存在しているかどうかモニタする接点が追加されました。これは自己モニタ用接点ブロックと呼ばれます。これは、接点ブロックがパネル上の正しい位置にカチッとはまると閉じるスプリング駆動式接点で構成されます。

ロープ型スイッチ

コンベアなどのマシンの場合、通常は、非常停止装置として危険領域に沿ってロープ型装置を設置するのが、より便利で効果的です。これらの装置は、プルスイッチをラッチするために鋼線ロープを使用しているので、その全長のどの位置でも、どの方向にでもロープを引いてスイッチをトリップし、マシン電源を遮断できます。

ロープ型スイッチは、ケーブルが引かれたことだけでなく、ケーブルがたるんだときも検知する必要があります。たるみの検知によりケーブルの切断も確実に検知できます。

スイッチの性能は、ケーブルの距離に影響されます。距離が短い場合は安全スイッチを一方の端に取付け、もう一方の端にはテンションスプリングを取付けます。距離が長い場合は安全スイッチをケーブルの両端に取付け、オペレータの1つの動作で停止コマンドを起動できるようにします。ケーブルを引くのに必要な力は、200N (45ポンド)以下、またはケーブルサポート間の中央で400mm (15.75インチ)以下の距離でなければなりません。

両手用制御

両手用制御(バイマニュアル制御とも呼ばれる)の使用は、マシンが危険な状態のときに接近するのを防ぐ一般的な方法です。マシンを稼働させるために、同時に(互いに0.5秒以内) 2つの始動ボタンを操作することが必要です。これは、オペレータの両手が安全な位置(すなわち制御ユニット)に置かれていること、したがって危険な領域にはないことを確認できます。制御は、危険な状況にあっても動作を継続する必要があります。マシンの動作は、制御ユニットのいずれかが開放されたら停止する必要があり、一方の制御ユニットが開放された場合は、もう一方の制御ユニットも開放されてから機械を再始動できます。

両手用制御システムは、制御機器とあらゆるフォルトを検出するモニタシステムの整合性に大きく関わってきます。したがって、この方法は、正確な仕様に沿って設計することが重要です。両手用制御安全システムの性能は、次のようにISO 13851 (EN 574)のタイプに位置付けられ、ISO 13849-1のカテゴリに関連付けられます。機械安全に使用される最も一般的なタイプは、IIIBとIIICです。以下の表に、安全性能のタイプとカテゴリの関係を表します。

要件	タイプ				
	I	II	III		
			A	B	C
同期動作			X	X	X
カテゴリ1の使用(ISO 13849-1から)	X		X		
カテゴリ3の使用(ISO 13849-1から)		X		X	
カテゴリ4の使用(ISO 13849-1から)					X

物理的な設計では、不適切な操作(例えば、手と肘を使うなど)を回避する必要があります。これは、距離をとるかまたはシールドを行なうことで可能です。両方のボタンを解除してから、再度押さない限り、マシンが1つのサイクルから次のサイクルへ進まないようにする必要があります。この方法でマシンが稼働を続けている状態で、両方のボタンが閉塞する可能性を回避できます。いずれかのボタンを解除すると、マシンが停止する必要があります。

両手用制御機器の使用では、一部対応しきれない危険が残る場合が多いので、十分な考慮が必要です。しかし、他の保護装置と組み合わせて使用した場合、保護レベルが向上するので、ティーチモードのペンダント型または寸動型制御機器などの用途には非常に有効です。

ISO 13851 (EN574)に、両手用制御の追加のガイダンスを提供しています。

イネーブルスイッチ

イネーブルスイッチは、オペレータがイネーブルスイッチを作動位置にしている間だけは、危険部分を稼働させたまま危険領域に入れるようにする制御装置です。イネーブルスイッチには2点式または3点式スイッチが使用されます。2点式スイッチは、アクチュエータが動作していないときはオフになり、動作中はオンになります。3点式スイッチは、動作していないときはオフ(1の位置)、中央の位置にあるときはオン(2の位置)、アクチュエータが中央の位置を超える位置に動かされるとオフ(3の位置)になります。さらに、3の位置から1の位置に戻すと、2の位置を通過しても出力回路は閉じません。

イネーブルスイッチは、他の安全関連機能と組み合わせて使用する必要があります。典型的な例では、動作を制御された低速モードにします。スローモードにすると、オペレータはイネーブルスイッチを保持したまま危険領域に入ることができます。

イネーブルスイッチを使用しているときは、信号はイネーブルスイッチがアクティブであることを示さなければなりません。

ロジックデバイス

ロジックデバイスは、制御システムの安全関連部分で中心的な役割を果たします。ロジックデバイスは安全システムのチェックとモニタを行ない、機械の始動を許可したり、機械を停止するコマンドを実行したりします。

機械に必要な複雑性や機能性に合った安全構造を作成できるように幅広いロジックデバイスがそろっています。安全機能を完備するために専用の論理装置が必要な小型の機械では、小型のハード配線式モニタ用セーフティリレーが最も経済的です。モジュール式および構成可能なモニタ・セーフティ・リレーは、大規模で、多種多様な安全保護装置と最小限のゾーン制御が要求される場合に適しています。中規模以上のより複雑な機械には、分散I/Oを使用したプログラマブルシステムが適しています。

モニタ・セーフティ・リレー

モニタ・セーフティ・リレー(MSR)モジュールは、さまざまな安全システムで重要な役割を果たします。通常、これらのモジュールは、安全機能を確実に動作させるための追加の回路を構成する2つ以上の強制開離式リレーで構成されています。

強制開離式リレーは、専用の「アイスキューブ」リレーです。ポジティブガイド式リレーはEN50025の性能要件を満たさなければなりません。基本的に、これらは通常閉接点と通常開接点が同時に閉じるのを防ぐように設計されています。最近の設計では、電気機械式出力が安全基準を満たすソリッドステート出力に変更されています。

モニタ・セーフティ・リレーは、安全システムで多くのチェックを実行します。電源投入時に、内部コンポーネントの自己チェックを実行します。入力装置が作動すると、MSRが冗長入力の結果を比較します。問題がなければ、MSRは外部アクチュエータをチェックします。これが正常な場合、MSRはリセット信号を待ってから、出力を有効にします。

適切なセーフティリレーは、モニタする装置のタイプ、リセットのタイプ、出力の数とタイプなど、さまざまな要素に基づいて選択します。

入力タイプ

安全ガード装置は、何が起こったかをさまざまな方法で通知します。

接触型インターロックおよび非常停止：機械的な接点は、1つの通常閉接点があるシングルチャネルかまたは両方とも通常閉接点のデュアルチャネルです。MSRはシングルまたはデュアルチャネルに対応し、デュアルチャネル配列についてはクロスフォルト検出が可能でなければなりません。

非接触型インターロックおよび非常停止：機械的な接点は、デュアルチャネルで、1つの通常開と1つの通常閉接点があります。MSRは、多様な入力を処理できなければなりません。

出力ソリッドステート切換えデバイス：ライトカーテン、レーザスキャナ、ソリッドステート非接触型には2つのソース出力があり、独自にクロスフォルト検出を実行します。MSRは、デバイスのクロスフォルト検出手段を無視できなければなりません。

感圧式マット：マットは、2つのチャネル間で短絡します。MSRは、繰返される短絡に耐えられなければなりません。

感圧式エッジ：エッジの中には、4線式マットのように設計されているものがあります。また、抵抗を変えられる2線式デバイスもあります。MSRは、短絡または抵抗の変化を検出できなければなりません。

電圧：停止中のモータのバックEMFを測定する。MSRは、高電圧に耐えられるだけでなく、モータのスピンダウンに伴う電圧低下を検出できなければなりません。

停止動作：MSRは、さまざまな冗長センサからのパルスストリームを検出しなければなりません。

両手用制御：MSRは、通常開および通常閉のさまざまな入力を検出し、0.5秒を計時して、ロジックを処理できなければなりません。

モニタ・セーフティ・リレーは、異なる電気特性を持つこれらのタイプのデバイスの互いにインターフェイスするように特別に設計されていなければなりません。一部のMSRは複数の異なるタイプの入力に接続できますが、デバイスを選択すると、MSRはそのデバイスとしかインターフェイスできなくなります。設計者は、その入力デバイスと互換性のあるMSRを選択する必要があります。

入力インピーダンス

モニタ・セーフティ・リレーの入力インピーダンスはそのリレーに入力デバイスをいくつ接続できるか、その入力装置をどのくらい離れた場所に取付けることができるかを決定します。例えば、セーフティリレーの許容可能な最大入力インピーダンスが500Ωだとします。入力インピーダンスが500Ωより大きいときは、出力をオンしません。ユーザは、入力インピーダンスが以下に示す最大仕様値未満に収まっているように注意しなければなりません。使用するワイヤの長さ、サイズおよびタイプが、入力インピーダンスに影響します。

入力デバイスの数

モニタ・セーフティ・リレーMSRのユニットに接続する入力デバイスの数と、その入力デバイスをチェックする頻度を決めるときは、リスクアセスメントのプロセスを使用する必要があります。非常停止およびゲートインターロックを常に操作可能な状態に保つには、リスク評価で決められた間隔で、定期的に動作をチェックする必要があります。例えば、マシンサイクルごとに(例えば、1日に数回)開かれるインターロックゲートに接続されたデュアルチャネル入力MSRUは、チェックする必要はありません。なぜなら、ガードを開くと、MSRUが自己チェックを行ない、入力および出力(構成によって異なる)に単一フォルトがないか確認するからです。ガードが開く頻度が高くなれば、チェック処理の整合性も高くなります。

次に、非常停止(E-Stop)の例を紹介します。通常、非常停止は、非常停止にのみ使用されるので、使用されることはめったにありません。したがって、定期的に非常停止を使用して、効果を確認するためのプログラムを確立する必要があります。3番目の例は、機械調整用の点検窓ですが、これも非常停止と同じで、めったに使用されません。そこで同じように、定期的に非常停止を使用するプログラムを確立する必要があります。

リスクアセスメントは、入力装置のチェックが必要かどうか、どのくらいの頻度でチェックすればよいかを決定するために役立ちます。リスクのレベルが高くなれば、チェック処理に求められる整合性もさらに高くなります。さらに、「自動」チェックの頻度が低くなれば、その分だけ頻繁に「手動」チェックを実施する必要があります。

入力クロスフォルト検出

デュアル・チャネル・システムでは、入力デバイスのチャネル間の短絡フォルト(クロスフォルトとも呼ばれる)を安全システムで検出できなければなりません。このために、検知装置またはモニタ・セーフティ・リレー(MSR)を使用します。

ライトカーテン、レーザスキャナ、および高度な非接触型センサなどのマイクロプロセッサベースのモニタ・セーフティ・リレーは、これらの短絡をさまざまな方法で検出します。クロスフォルト検出の一般的な方法では、さまざまなパルステストを使用します。出力信号は、非常に早いパルスです。チャネル1のパルスは、チャネル2のパルスからオフセットされています。短絡が発生すると、パルスが同時に発生し、デバイスによって検出されます。

電気機械式のモニター・セーフティ・リレーでは異なるダイバーシティ技術を採用しています。すなわち、プルアップ入力を1つとプルダウン入力を1つ使用しています。チャネル1からチャネル2の間の短絡は、過電流保護装置をアクティブにし、安全システムをシャットダウンします。

出力

MSRの出力の数は決まっていません。出力のタイプで、特定のアプリケーションに使用するMSRを選択することができます。

ほとんどのMSRには直ちに動作する安全出力が少なくとも2つあります。MSRの安全出力は、通常開の特性を持ちます。これらは冗長性と内部チェック機能を持つため安全定格されます。もう一種類の出力は遅延出力です。遅延出力は、通常、カテゴリ1の停止で使用されます。カテゴリ1の停止では、危険箇所へのアクセスを許可する前に、機械が停止機能を実行するために時間がかかります。MSRには補助出力もあります。一般的には、補助出力は通常閉と見なされます。

出力定格

出力定格は、安全保護装置が負荷を切換える能力を表します。通常、産業用装置の定格は、負荷抵抗または電磁負荷として示されます。負荷抵抗は、ヒータ・タイプ・エレメントであることが多く、電磁負荷は通常、リレー、コンタクタ、またはソレノイドです。この場合、負荷の誘導特性が大きくなります。規格IEC 60947-5-1の付録Aは、負荷の定格を示します。これは、セーフティカタログの「原理」の項にも示しています。

指定文字：指定は先頭の文字で、その後に数字が続きます。例えばA300のようになります。文字は、従来の密閉型熱電流と、電流が直流(DC)か交流(AC)であるかに関連します。例えば、Aは10A交流電流(AC)を示します。数字は、定格絶縁電圧を示します。例えば、300は300Vを表します。

用途：用途とは、装置が切換えることになる負荷のタイプを説明します。IEC 60947-5に関連する用途を以下の表に示します。

用途	負荷の説明
AC-12	抵抗負荷と、光カプラで絶縁されたソリッドステート負荷の制御
AC-13	トランス絶縁付きのソリッドステート負荷の制御
AC-14	わずかな電磁負荷(72 VA未満)の制御
AC-15	72VAを超える電磁負荷
DC-12	抵抗負荷と、光カプラで絶縁されたソリッドステート負荷の制御
DC-13	電磁の制御
DC-14	回路内にエコノミレジスタがある電磁負荷の制御

熱電流Ith：従来の密閉型熱電流は、指定したエンクロージャに取付けられたときの、装置の温度上昇テストに使用される電流の値です。

定格動作電圧Ueおよび定格動作電流Ie：定格動作電流と電圧は、通常の動作条件におけるスイッチエレメントのメイクおよびブレークの容量を指定します。アレン・ブラドリーのGuardmaster製品は、厳密にAC125V, AC250V, およびDC24Vに定格されています。指定された定格以外の電圧での使用に関しては、工場に問い合わせてください。

VA：VA (Voltage x Amperage)定格は、回路をメイクするときと、回路をブレークするときのスイッチエレメント定格を示します。

例1：A150, AC-15定格は、この接点が7200VAの回路をメイクできることを示します。AC120Vでは、接点は60Aの突入回路をメイクできます。AC-15は電磁負荷なので、60Aは短期間(電磁負荷の突入電流)のみに限られます。回路のブレークは720VAだけです。これは、電磁負荷の定常状態電流は6Aで、これは定格動作電流だからです。

例2：N150, DC-13定格は、この接点が275VAの回路をメイクできることを示します。AC125Vでは、接点は2.2Aの回路をメイクできます。DCの電磁負荷にはAC電磁負荷のような突入電流はありません。回路のブレークも275VAです。これは、電磁負荷の定常状態電流は2.2Aで、これは定格動作電流だからです。

マシンの再起動

例えば、稼動中のマシンでインターロックガードが開いた場合、セーフティ・インターロック・スイッチが機械を止めます。ほとんどの場合、ガードが閉じてすぐに機械が再始動しないのは、当然のことです。これを実現する一般的な方法では、ラッチ機能付きコンタクタの開始処理を使用します。

始動ボタンを押してから離すと、電源接点を閉じているコンタクタの制御コイルがすぐに出力状態になります。電源接点に電力が供給されている限り、電源接点と機械的にリンクされているコンタクタの補助接点によって、制御コイルは出力状態(電気的にラッチされた状態)に保たれます。主電源または制御電源が遮断されると、コイルがオフ状態になり、主電源と補助接点が開きます。ガードのインターロックは、コンタクタの制御回路に配線されています。つまり、再始動するには、ガードを閉じてから通常の始動ボタンでスイッチを「オン」にして、コンタクタをリセットし機械を起動します。

通常のインターロック状態に関する要件は、ISO 12100-1の第3.22.4項で明確にされています。

“ガードが閉じている場合、ガードで覆われている機械の危険な機能は動作可能であるが、ガードを閉じる行為そのもので動作が開始されることはない。”

ほとんどの機械が、前述のように動作する1つまたは2つのコンタクタをすでに備えています(または、同じ結果になるシステムを備えています)。既存の機械にインターロックを取付けるときは、電源制御の配置がこの要件を満たしているか判断し、必要に応じて追加措置を取る必要があります。

リセット機能

アレン・ブラドリーのGuardmasterモニタ・セーフティ・リレー(MSR)は、モニタ付き手動リセットまたは自動/手動リセットのいずれかを備えるように設計されています。

モニタ付き手動リセット

モニタ付き手動リセットでは、ゲートが閉じるか、非常停止がリセットされた後、回路をいったん閉じてから開く必要があります。機械的にリンクされた電源切換えコンタクタの通常閉の補助接点は、モメンタリ式押しボタンと直列に接続されます。ガードが開いてから再度閉じた後に、セーフティリレーはリセットボタンを押してから離すまで、機械が再始動できないようにします。これは、EN ISO 13849-1に指定された追加の手動リセットの要件の意図を満たします。例えば、リセット機能は、両方のコンタクタがオフで、両方のインターロック回路(そして、それに伴ってガード)が閉じていること、また、(状態の変化が必要であるため)リセットアクチュエータがどのような形でもバイパスされないか、またはブロックされないことを保証します。これらのチェックが成功すると、機械が通常の制御から再起動できます。EN ISO 13849-1は、オン状態からオフするには状態の変化を必要としますが、反対の効果でも同じ保護原則を達成することができます。

リセットスイッチは、危険がよく見える場所に配置し、オペレータが、操作する前にその領域がクリアされたことをチェックできるようにする必要があります。

自動/手動リセット

セーフティリレーの中には、自動/手動リセットを備えているものもあります。手動リセットモードはモニタされず、ボタンが押されたときにリセットが行なわれます。リセットスイッチが短絡またはジャムしていても検出されません。この方法では、追加の手段を使用しない限り、EN ISO 13849-1に指定された追加の手動リセットの要件を達成できません。

この場合、自動リセットが可能になるように、リセットラインにジャンパを使用できます。ユーザは、ゲートが閉じたときに機械が起動しないようにするために、別の手段を採用する必要があります。

自動リセット装置には、手動スイッチ操作は不要ですが、動作を止めた後、システムをリセットする前に、システムの整合性チェックを必ず実行します。自動リセット装置は、リセット機能のない装置とは異なります。後者では、安全システムは動作を止めた後、直ちに有効になり、システムの整合性チェックは行なわれません。

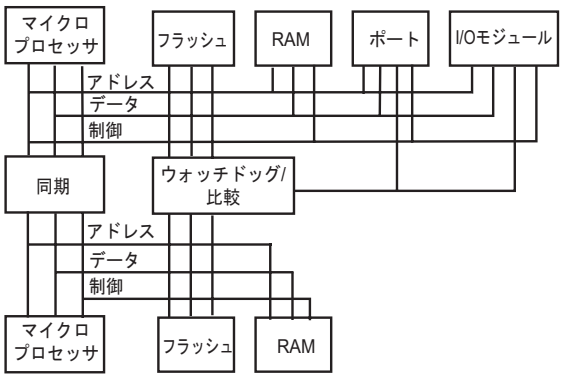
リセットスイッチは、危険がよく見える場所に配置し、オペレータが、操作する前にその領域がクリアされたことをチェックできるようにする必要があります。

制御ガード

制御ガードは、ガードが開くとマシンを停止し、ガードが閉じると再度直接マシンを起動します。いかなる場合でも予想できない起動や、停止の失敗は非常に危険であるため、制御ガードの使用は特定の強制的な状況の下でのみ許されます。インターロック装置には最高の信頼性が必要です(通常はガードロックの使用をお奨めする)。制御ガードの使用を検討できるのは、ガードが閉じている間、オペレータの体またはその一部が危険領域内に留まったり、近づいたりする可能性のないマシンの場合だけです。制御ガードは、危険領域への唯一の接近方法でなければなりません。

セーフティ・プログラマブル・ロジック・コントローラ

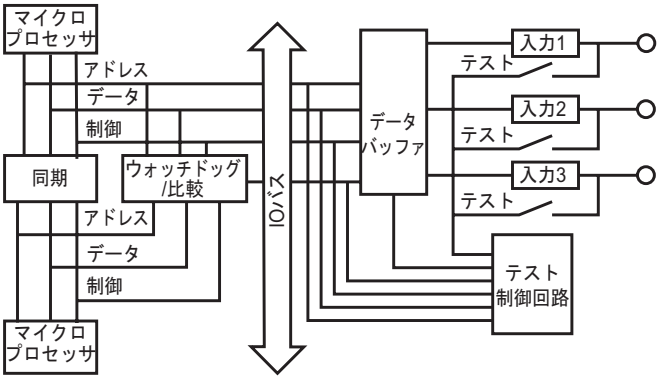
柔軟でスケーラブルな安全アプリケーションに対する要望がセーフティPLC/コントローラ開発の機動力となっています。プログラマブル・セーフティ・コントローラは、安全アプリケーションでも、使い慣れている標準のプログラマブルコントローラと同じくらい自由な制御を可能にします。ただし、標準のPLCとセーフティPLCには大きな違いがあります。以下の図に示すように、セーフティPLCには、より複雑な安全システムのスケーラビリティ、機能、統合要件に対応するためにさまざまなプラットフォームが用意されています。



1oo2Dアーキテクチャ

I/O、メモリ、および安全通信を処理するために複数のマイクロプロセッサが使用されています。ウォッチドッグ回路は診断分析を実行します。このタイプの構造は、2つのマイクロプロセッサのいずれかが安全機能を実行し、両方のマイクロプロセッサが確実に同期をとって動作するように拡張診断が実行されるため、1oo2Dと呼ばれています。

さらに、各入力回路は毎秒何回も内部的にテストされ、正しく動作していることを確認されます。以下の図に、入力のブロックダイアグラムを示します。非常停止は月に1回押されるだけかもしれませんが、回路は継続的にテストされているので、実際に押されたときは、非常停止はセーフティPLC内部で正しく感知されます。



安全入力モジュールのブロックダイアグラム

セーフティPLC出力は、電気機械式または安全定格のソリッドステートです。入力回路と同様に、出力回路も毎秒複数回のテストが行なわれ、出力をオフにできることが確認されます。3つの回路のいずれか1つが故障した場合は、他の2つの回路によって出力がオフにされ、内部モニタ回路によってフォルトが報告されます。

安全デバイスに機械的な接点(E-stop、ゲートスイッチなど)を使用しているときは、ユーザはパルステスト信号を適用してクロスフォルトを検出できます。高価な安全出力の使用を回避するために、ほとんどのセーフティPLCは機械的接点装置に接続できる特定のパルス出力を提供します。

ソフトウェア

セーフティPLCのプログラムは、標準PLCとほとんど同じようにプログラムされます。前述の追加された診断とエラーチェック機能は、すべてオペレーティングシステムによって実行されます。プログラマはこれらが行なわれていることに気づきません。ほとんどのセーフティPLCには、安全システム用のプログラムを作成するために使用される特殊な命令があり、これらの命令はセーフティリレーに対応する機能に似ています。例えば、非常停止(Emergency Stop)命令は、MSR 127とほとんど同じように機能します。これらの命令の陰にあるロジックは複雑ですが、プログラマは単純にこれらのブロックをつなぎ合わせるだけなので、安全プログラムは比較的シンプルに見えます。これらの命令は、他のロジック、計算、データ操作などと組み合わせると、その動作が適用される規格に確実に適合することを第三者機関によって保証されます。

ファンクションブロックは、安全機能をプログラミングするための優れた方法です。ファンクションブロックとラダーロジックに加え、セーフティPLCには、認定された安全アプリケーション命令があります。認定済みの安全命令によりアプリケーション固有の動作が可能になります。この例では、非常停止命令を示します。ラダーロジックで同じ機能を実行するには、ラダーロジックのラングが約16必要になります。ロジックの動作は非常停止命令に埋め込まれるため、埋め込まれたロジックはテストする必要がありません。

認可ファンクションブロックは、ほとんどすべての安全装置と接続できます。この中に含まれないのは、抵抗技術を使用するセーフティエッジです。

セーフティPLCはPLCは、変化が起きたかどうかを追跡する機能の署名を生成します。この署名は、通常、プログラム、I/O構成、およびタイムスタンプが組み合わされています。プログラムのファイナライズと妥当性確認が行なわれるときは、この署名を後で参照できるように妥当性確認の結果の一部として記録する必要があります。プログラムの変更が必要になった場合は、再度妥当性確認が必要で、新しい署名を記録する必要があります。プログラムはパスワードでロックして、不正に変更されるのを防ぐこともできます。

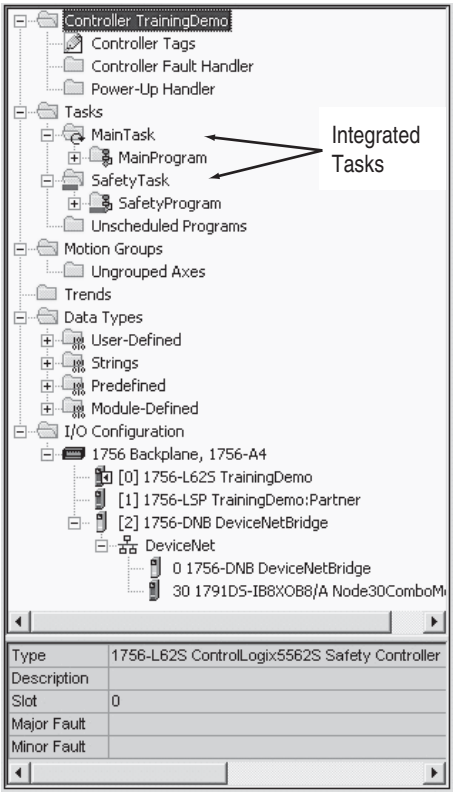
プログラマブル・ロジック・システムを使用すると、モニタ・セーフティ・リレー(MSR)と比べて配線がシンプルになります。MSR上の特定の端子への配線と異なり、入力デバイスは任意の入力端子に接続され、出力デバイスは任意の出力端子に接続されます。その後、ソフトウェアによって端子が割付けられます。

統合セーフティコントローラ

安全制御ソリューションは、安全と標準の制御機能が混在して共に動作できる1つの制御アーキテクチャに完全に統合されています。モーション、ドライブ、プロセス、バッチ、高速シーケンシャル、およびSIL 3安全を1台のコントローラで実行する能力には、大きな利点があります。安全制御と標準制御を統合することで、共通のツールと技術を使用して、設計、導入、実施、および保守に関わるコストを削減できる可能性が生まれます。安全ネットワーク上で共通の制御用ハードウェア、分散型セーフティI/Oまたはデバイスを使用できたり、共通のHMIデバイスを使用できることで、購入コストと保守費用を削減でき、開発期間も短縮できます。各機能の共通性により、生産性を向上させ、問題のトラブルシューティング時間を短縮し、トレーニングコストを低減することができます。

以下の図に、制御と安全保護の統合の例を示します。安全関連ではない標準の制御機能はメインタスクに組み込まれます。安全関連の機能は、安全タスクに組み込まれます。

標準と安全関連機能は、すべて互いに分離されています。例えば、安全タグは標準ロジックで直接読取ることができます。安全タグは、EtherNet、ControlNetまたはDeviceNet上のGuardLogixコントローラ間で交換できます。安全タグのデータは、外部デバイス、ヒューマン・マシン・インターフェイス(HMI)、パーソナルコンピュータ(PC)または他のコントローラを使用して直接読取ることができます。



1. 標準タグとロジックは、ControlLogixと同様に動作します。

2. 標準タグデータ(プログラム用またはコントローラ用)、および外部デバイス、HMI、PC、その他のコントローラなど

3. 統合コントローラであるGuardLogixは、標準のタグデータを安全タスク内で使用するために安全タグに移動(マップ)することができます。これは、GuardLogixの標準側からステータス情報を読取れるようにすることを目的としています。このデータは、安全出力を直接制御するために使用することはできません。

4. 安全タグは標準ロジックで直接読取ることができます。

5. 安全タグは安全ロジックで読み書きできます。

6. 安全タグは、EtherNetを介してGuardLogixコントローラ間でやり取りすることができます。

7. 安全タグデータ(プログラム用またはコントローラ用)は、外部デバイス、HMI、PC、その他のコントローラなどで読取ることができます。一度このデータを読取ると、安全データではなく、標準データと見なされることに注意してください。

安全ネットワーク

これまでプラントフロアの通信ネットワークは、製造メーカに対して柔軟性を向上させ、診断機能を改善し、距離を伸ばし、導入および配線のコストを削減し、保守を容易にし、製造作業の生産性を総合的に改善してきました。これらと同じ動機で、産業用安全ネットワークも実現に向けて動いています。安全ネットワークを使用すると、安全I/Oと安全デバイスを1本のネットワークケーブルを使用して機械の周囲に分散させることができるため、導入コストを削減すると同時に、診断を改善し、より複雑な安全システムを実現できるようになります。また、セーフティPLC/コントローラ間で安全な通信が可能になり、複数のインテリジェントシステム間に安全制御を分散させることができるようになります。

安全ネットワークは通信エラーの発生を抑えるわけではありません。安全ネットワークは転送エラーの検出能力に優れているため、安全デバイスが適切な処置を行なえるようになります。検出される通信エラーには、メッセージの挿入、メッセージの損失、メッセージ不正、メッセージ遅延、メッセージの重複、メッセージのシーケンスエラーなどがあります。

ほとんどのアプリケーションでは、エラーが検出されるとデバイスは既知の電源が断たれた状態(一般的に安全状態と呼ばれる)になります。安全入力または出力デバイスは、このような通信エラーの検出に関与しているので、適切な場合は安全状態になります。

初期の安全ネットワークは、特定のメディアタイプやメディアアクセス方法に縛られていたので、製造メーカは安全機能の一部になる特別なケーブル、ネットワーク・インターフェイス・カード、ルータ、ブリッジなどを使用する必要がありました。これらのネットワークは、安全デバイス間の通信のみに対応していました。したがって、メーカは機械制御ストラテジに2つ以上のネットワーク(標準制御用に1つと、安全関連制御用に1つ)を使用する必要があったので、設置、トレーニング、スペアパーツに多くのコストがかかりました。

最近の安全ネットワークは、1本のネットワークケーブルを安全制御装置と標準の制御装置のいずれかの通信にも使用できます。CIP (Common Industrial Protocol：共通の産業プロトコル) Safetyは、ODVA (Open DeviceNet Vendors Association)によって公開されているオープン規格のプロトコルで、DeviceNet, ControlNet, およびEtherNet/IPネットワーク上の安全装置間の安全通信に使用できます。CIP Safetyは標準のCIPプロトコルを拡張したプロトコルで、安全装置と標準装置をすべて同じネットワーク上に置くことができます。安全装置を含むネットワーク間をブリッジすることも可能なため、安全装置を再分割して安全機能の応答時間を微調整できたり、安全装置の配置が容易になったりします。安全プロトコルは末端装置(セーフティPLC/コントローラ、セーフティI/Oモジュール、安全構成部品)にだけ関与しているので、標準のケーブル、ネットワーク・インターフェイス・カード、ブリッジ、およびルータが使用され、特殊なネットワークハードウェアは必要なく、これらの装置を安全機能から排除することができます。

出力デバイス

セーフティ制御リレーおよびセーフティコンタクタ

制御リレーおよびコンタクタは、アクチュエータから電力を取り除くために使用されます。安全定格を与えるために、制御リレーとコンタクタに特殊機能が追加されています。

機械的にリンクされた通常閉接点は、制御リレーおよびコンタクタのステータスをロジックデバイスにフィードバックするために使用されます。機械的にリンクされた接点を使用すると、安全機能が確保されます。機械的にリンクされた接点の要件を満たすために、通常閉接点と通常開接点を同時に閉状態にすることはできません。IEC 60947-5-1は、機械的にリンクされた接点の要件を定義しています。通常開接点が溶着した場合は、通常閉接点は0.5mm以上開いたままになります。これとは逆に通常閉接点が溶着した場合は、通常開接点が開いたままになります。

安全システムは、特定の位置からのみ開始されなければなりません。標準定格の制御リレーとコンタクタは、接極子を押して通常開接点を閉じることができます。安全定格デバイスでは、予期しない起動を緩和するために、アマチャは手動制御されないように保護されています。

セーフティ制御リレーでは、通常閉接点はメインスパナで動かされます。セーフティコンタクタはアダーデッキを使用して機械的にリンクされた接点の場所を確認します。接点ブロックがベースから落ちた場合は、機械的にリンクされた接点は閉じたままになります。機械的にリンクされた接点は、セーフティ制御リレーまたはセーフティコンタクタに永久的に固定されます。大型のコンタクタでは、幅の広いスパナの状態を正確に反映させるには、1つのアダーデッキでは不十分です。ミラー接点がコンタクタの片側に配置されます。

制御リレーまたはコンタクタのドロップアウト時間は、安全距離の計算に関わってきます。通常、コイルにサージサプレッサが取付けられているときは、コイルを動かす接点の寿命が延びます。AC電源用コイルでは、ドロップアウト時間に影響しません。DC電源用コイルでは、ドロップアウト時間が増加します。増加量は選択した抑制のタイプによって異なります。

制御リレーおよびコンタクタはは、大きな電流負荷を0.5Aから100A以上に切換えるように設計されています。安全システムは低電流で動作します。安全システムのロジックデバイスによって生成されるフィードバック信号は、通常DC24Vで約数mAから数十mAになります。セーフティ制御リレーとセーフティコンタクタは金めっきされた分岐接点を使用して、より低い電流切換えの信頼性を向上させます。

過負荷保護

電気規格と地域の建築基準法では、モータの過負荷保護が要求されます。過負荷保護装置の診断機能は、装置とオペレータの安全を強化します。現在使用可能なテクノロジでは、過負荷、位相損失、地絡、ストール、ジャム、負荷不足、電流の不均衡、および過熱などのフォルト状態を検出できます。トリップする前にフォルトを検出して通知することにより、生産可能時間を拡大し、オペレータや保守要員を危険な状態から保護することができます。

ドライブおよびサーボ

安全定格ドライブおよびサーボは回転エネルギーが流出するのを回避し、非常停止だけでなく安全停止を実行するためにも使用されます。

ACドライブは、ゲート制御回路から電力を除去するために冗長チャネルを使用して、安全定格を確保しています。1つのチャネルはイネーブル信号です。これは、ゲート制御回路の入力信号を除去するハードウェア信号です。もう1つのチャネルは、ゲート制御回路から電力を除去する強制開離リレーです。強制開離リレーは、ロジックシステムに状態信号も返します。この冗長機能によって、コンタクタを使用しなくても安全関連ドライブを非常停止回路に適用できるようになります。

サーボは、安全機能を実現するために冗長安全信号を使用してACドライブと同様の結果を出します。1つの信号はゲート制御回路の駆動力を遮断します。もう1つの信号は、ゲート制御回路の電源に送られる電力を遮断します。2つの強制開離リレーは、信号を除去し、ロジックデバイスにフィードバックを送るためにも使用されます。

接続システム

接続システムには、安全システムの設置と保守費用を低減するという付加価値があります。設計時には、シングルチャネル、デュアルチャネル、デュアルチャネル(表示付き)、さまざまなタイプのデバイスを考慮する必要があります。

デュアル・チャネル・インターロックを直列に接続する必要がある場合は、分散型ブロックを使用すると設置がシンプルになります。IP67定格の場合は、このタイプのボックスを離れた場所にある機械に取付けることができます。多種多様な装置を組み合わせて使用する場合は、ArmorBlock Guard I/Oボックスを使用できます。入力はソフトウェアを使用して、さまざまなタイプのデバイスに対応できるように構成できます。

安全距離の計算

危険箇所はオペレータが到達する前に安全な状態になる必要があります。安全距離の計算に関しては、2つの規格グループが優勢になっています。これらの規格は、次のようにグループ化されます。

ISO EN: (ISO 13855およびEN 999)

米国/カナダ(ANSI B11.19, ANSI RIA R15.06およびCAN/CSA Z434-03)

式

最小安全距離は、停止コマンドの処理に必要な時間と、検出されるまでにオペレータが検出領域に侵入できる距離で決まります。世界中で同じ形式および要件を持つ式が使用されます。ただし、変数を表すために使用される記号と測定の単位は異なります。

以下の式を使用します。

ISO EN: $S = K \times T + C$

US CAN: $Ds = K \times (Ts + Tc + Tr + Tbm) + Dpf$

この場合、DsおよびSは、危険な領域から一番近い検出ポイントまでの最小安全距離です。

接近する方向

ライトカーテンまたはエリアスキャナが使用されている場合に安全距離の計算を行なうときは、検出装置への接近方法を考慮する必要があります。接近方法として次の3つが考えられます。

通常：検出面に垂直方向から接近する。

水平：検出面と平行に接近する。

斜め：検出領域に斜めの方向から接近する。

速度定数

Kは、速度定数です。速度定数の値は、オペレータの動き(手の速度、歩く速度、歩幅)によって異なります。このパラメータは、調査データに基づいて、オペレータが停止しているときの手の速度は1600mm/sec (63インチ/sec)と想定するのが妥当とされています。実際のアプリケーションの状況を考慮する必要があります。一般的なガイドラインとして、接近速度は1600～2500mm/sec (63～100インチ/sec)の範囲で変化します。適切な速度定数は、リスクアセスメントによって決定します。

停止時間

Tは、システムが完全に止まるまでの時間です。つまり、停止信号の開始から危険が解消するまでの合計時間を秒(sec)単位で表します。この時間は、分析しやすくするために、増加部分(Ts, Tc, Tr, およびTbm)に細分化します。Tsは期待する最低限のマシン/装置の停止時間です。Tcは、最期待する最低限の制御システムの停止時間です。Trは、インターフェイスを含む安全保護装置の応答時間です。Tbmは、エンドユーザが予め設定した停止時間の制限を超えたことをブレーキモニタが劣化として検出するまでに猶予される追加の時間です。Tbmは部分回転機械プレスに使用されます。Ts + Tc + Trの値がわからない場合、通常は停止時間測定装置を使って測定されます。

奥行侵入係数

奥行侵入係数は、CとDpfという記号で表されます。これは、安全保護装置によって検出されるまでに危険箇所に向かう最大移動距離です。奥行侵入係数は、装置の種類とアプリケーションによって異なります。最適な奥行侵入係数を決定するには、適切な基準を調べる必要があります。ライトカーテンやエリアスキャナへの垂直方向からの接近の場合、対象物感度は64mm (2.5インチ)未満なので、ANSIおよびカナダ規格では、次の式を使用します。

Dpf = 3.4 x (対象物感度 - 6.875mm) (ただし、負の数でない)

ライトカーテンまたはエリアスキャナへの垂直方向からの接近の場合、対象物感度は40mm (1.57インチ)未満なので、ISOおよびEN規格では、次の式を使用します。

C = 8 x (対象物感度 - 14mm) (ただし、負の数でない)

これら2つの式は、19.3mmで交差します。対象物感度が19mm未満の場合、ライトカーテンまたはエリアスキャナを危険箇所からかなり遠ざける必要があるので、米国およびカナダの方法ではより厳しく制限されます。対象物感度が19.3mmを超える場合、ISO EN規格はより厳しくなります。世界中で使用される機械を製造するメーカは、両方の式における最悪の条件を考慮する必要があります。

通り抜けアプリケーション

より大きな対象物感度を使用するときは、米国CANおよびISO EN規格とでは奥行侵入係数と対象物感度が多少異なります。米国/カナダの値が900mmのとき、ISO EN値は850mmです。ISO EN規格で40～70mmが許される場合、米国/カナダ規格では最大600mmまで許されます。

手を伸ばすアプリケーション

どちらの規格も最下段ビームの高さは最低でも300mm以上でなければならないことで一致していますが、最上段ビームの最低の高さについては見解が異なります。ISO ENは900mmとしており、一方米国/カナダは1200mmとしています。最上段ビームの値は非現実的に思われます。これを通り抜けアプリケーションで考えると、最上段ビームの高さは、オペレータが立った状態で十分に通れる高さが必要です。オペレータが検知面の上に手を伸ばすことができる場合は、部分検知基準が適用されます。

シングルまたはマルチビーム

シングルまたはマルチの個別ビームについては、ISO EN規格で詳細に定義されています。表7に、床からのマルチビームの実用的な高さを示します。ほとんどの場合の奥行侵入は850mmで、シングルビームの場合は1200mmを使用します。これに比べて、米国/カナダでは、これを通り抜けの要件として考慮しています。シングルビームおよびマルチビームの上、下、側面からの侵入についてを常に考慮する必要があります。

ビーム数	床からの高さ：mm (インチ)	C - mm (インチ)
1	750 (29.5)	1200 (47.2)
2	400 (5.7), 900 (35.4)	850 (33.4)
3	300 (11.8), 700 (27.5), 1100 (43.3)	850 (33.4)
4	300 (11.8), 600 (23.6), 900 (35.4), 1200 (47.2)	850 (33.4)

距離の計算

ライトカーテンへの垂直方向からの接近の場合、ISO ENと米国/カナダ用の安全距離計算はほとんど同じですが、相違点もあります。垂直に取付けられた対象物感度が最大40mmのライトカーテンに垂直方向から接近する場合、ISO ENの方法は2段階で行なわれます。最初に速度定数に2000を使用してSを計算します。

S = 2000 x T + 8 x (d -1 4)

最小距離Sは、100mmです。

距離が500mmを超える場合は、Kの値を1600に減らすことができます。K=1600を使用すると、Sの最小値は500mmになります。

米国/カナダの方法は1段階で行なわれます：Ds = 1600 x T * Dpf

この式では、応答時間が560msec未満のとき、規格と5%より大きな違いができます。

斜めからの接近

ほとんどのライトカーテンとスキャナは、垂直(垂直方向からの接近)または水平(水平方向からの接近)に設置されます。これらの設置方法は、±5°以内の意図的な設計であれば、角度があるとは見なされません。角度が±5°を超えた場合は、リスクの可能性(距離が短すぎるなど)を考慮する必要があります。一般的に、参照面(床)との角度が30°を超えると垂直と考えられ、30°未満の場合は水平と考えられます。

セーフティマット

セーフティマットの場合、オペレータは歩いて接近し、セーフティマットは床に設置されていると仮定して、安全距離にはオペレータの速度と歩幅を考慮する必要があります。マット上の上のオペレータの1歩目は、1200mm (48インチ)になります。オペレータが壇上に上る場合は、段の高さの40%だけ奥行侵入係数を減らすことができます。

例

例：オペレータは14mmのライトカーテンに垂直方向から接近するものとします。ライトカーテンはダイオードサプレッサ付きのDC電源コンタクタに接続されているMSRに接続されています。この安全システムの応答時間Trは、20 + 15 + 95 = 130msecです。マシンの停止時間Ts+Tcは、170msecです。ブレーキモニタは使用しません。Dpf値は1インチで、Cの値は0です。これで以下のように計算します。

Dpf = 3.4 (14 - 6.875) = 1インチ(24.2mm)

Ds = K x (Ts + Tc + Tr + Tbm) + Dpf
Ds = 63 x (0.17 + 0.13 + 0) + 1
Ds = 63 x (0.3) + 1
Ds = 18.9 + 1
Ds = 19.9インチ(505mm)

C = 8 (14-14) = 0

S = K x T + C
S = 1600 x (0,3) + 0
S = 480mm (18.9インチ)

そのため、世界中で使用されるマシンの場合の、セーフティ・ライト・カーテンを取付ける危険箇所からの最小安全距離は、508mm (20インチ)になります。

予期しない電源投入の回避

予期しない電源投入の回避については、多くの規格が取り上げています。その例として、ISO 14118、EN 1037、ISO 12100、OSHA 1910.147、ANSI Z244-1、CSA Z460-05、およびAS 4024.1603に記述されています。これらの規格に共通する主旨は、予期しない電源投入の回避の第一の手段は、システムからエネルギーを除去し、システムをオフの状態にロックすることというものです。これは、マシンの危険領域に作業員が安全に入れるようにすることを目的としています。

ロックアウト/タグアウト

新たに製造されるマシンには、ロック可能なエネルギー絶縁デバイスの装備が求められます。この装置は、電気、水圧、空圧、重力、レーザなどあらゆるタイプのエネルギーに適用されます。ロックアウトはエネルギー絶縁デバイスをロックすることを意味します。このロックは、制御された状況で所有者または管理者によってのみ解除できるようにする必要があります。複数の作業員がマシンの操作を行なう場合、各自がそれぞれエネルギー絶縁デバイスをロックしなければなりません。また、ロックした人を識別できる必要があります。

米国では、ロック可能なデバイスが取付けられていない旧式のマシンに対して、ロックアウトのかわりにタグアウトを使用します。この場合、マシン電源がオフになるとタグが適用され、タグホルダがマシンに作用している間は、マシンが始動しないようにすべての関係者に警告します。1990年以降、マシンを変更するときは、ロック可能なエネルギー絶縁デバイスを組み込むアップグレードが要求されます。

エネルギー絶縁デバイスは、エネルギーの供給または放出を物理的に回避する機械的なデバイスです。これらのデバイスには、サーキットブレーカ、ディスコネクトスイッチ、手動操作のスイッチ、プラグとソケットの組み合わせ、または手動操作のバルブなどが含まれます。電気的絶縁デバイスは、接地されていない電源の導線をすべてスイッチを切換えて、電極が個別に作動できないようにします。

ロックアウトとタグアウトは、マシンの予期しない始動を回避することを目的としています。予期しない始動の原因としては、制御システムの故障、始動制御、センサ、コンタクタ、またはバルブの誤動作、遮断後の電力の回復、その他内部または外部からの影響が考えられます。ロックアウトまたはタグアウトプロセスの完了後は、エネルギーの損失を確認する必要があります。

安全絶縁システム

安全絶縁システムは、マシンに所定のシャットダウンを実行し、さらに機械への電源をロックオフする簡単な手段になります。この方法は、より大型のマシンや製造システム、特に複数のエネルギー源が中間レベルや離れた場所に存在している場合に有効に機能します。

負荷の切り離し

電気機器のローカル絶縁のために、遮断してロックアウトする必要のある装置の直前にスイッチを配置することができます。Bulletin 194Eロードスイッチは、絶縁とロックアウトの両方の機能を持つ製品の1例です。

トラップ・キー・システム

トラップ・キー・システムは、ロックアウトシステムを実装するためのもう1つの手段です。ほとんどのトラップ・キー・システムはエネルギー絶縁デバイスから始まります。プライマリキーでスイッチをオフにすると、機械の電気エネルギーがすべての未接地供給導体から同時に取り除かれます。その後プライマリキーを取り外して、機械に接触する必要のある場所に持って行きます。より複雑なロックアウト処理に対応するために、さまざまなコンポーネントを追加することができます。

ロックアウトの代替手段

ロックアウトとタグアウトは、マシンの修理またはメンテナンス中に使用する必要があります。通常の生産作業中のマシンへの介入には、安全保護装置が適用されます。修理/メンテナンスと通常の生産作業の違いは明確でないこともあります。

通常の製造作業中に行なわれる一部の小規模な調整や修理作業では、必ずしもマシンのロックアウトは必要ありません。例えば、材料の積み降ろし、小規模なツールの交換および調整、注油程度の修理、廃材の撤去などの作業です。これらの作業は、定期的に繰返される、生産施設を使用するために不可欠な作業です。作業には、効果的な保護を行なう安全保護装置などの代替手段が使用されます。安全保護装置としては、インターロックガード、ライトカーテン、セーフティマットなどが挙げられます。適切な安全定格ロジックデバイスおよび出力装置と組み合わせて使用することで、オペレータは通常の製造作業中や小規模な修理の際に、危険領域に安全に接近することができるようになります。

安全関連制御システム

はじめに

安全関連制御システム(SRCS)は、危険な状況の発生を回避するマシン制御システムの一部です。これは独立した専用システムのこともあれば、標準のマシン制御システムに統合されている場合もあります。

このシステムの複雑さは、電源コンタクタの制御巻線に直列に接続されたガード・ドア・インターロック・スイッチと非常停止スイッチのようなシンプルなシステムから、ソフトウェアとハードウェアを介して通信する単純なデバイスと複雑なデバイスの両方で構成された複雑なシステムまでさまざまです。

安全関連制御システムは、安全機能を実行するように設計されています。SRCSは、予想されるあらゆる状況で正常な動作を継続できる必要があります。その内容は、安全機能とは何か、これを達成するためのシステムの設計方法は、およびそれをいつ行なったか、どのように示すか?です。

安全機能

安全機能は、特定の危険に際してマシン制御システムの安全関連部品によって実行され、制御対象の装置を安全な状態に保持できるようにする機能です。安全機能が故障すると、装置の使用に関わる危険性が急に高くなります。すなわち、危険な状況になります。

マシンには、常に少なくとも1つの危険が伴います。危険な状況は人が危険に曝されたときに発生します。危険な状況が直接人に危害を及ぼすわけではありません。危険に曝された人が危険を認識できれば、けがを避けることができます。危険に曝された人が危険に気づかない場合や、予期しない始動によって危険な状況が発生する場合もあります。安全システム設計者の主な作業は、危険な状況や予期しない始動を回避することです。

安全機能は、通常、複数部分に分かれた要件で説明されています。例えば、インターロックガードによって起動される安全機能は、3つの部分から構成されてます。

1. ガードで保護された危険箇所は、ガードが閉じられるまで動作できません。

2. ガードを開くと、危険箇所がその時点で動作していた場合は、停止されます。

3. 防護ドアを閉じたとしても、ガードで保護された危険箇所は再始動しません。

特定のアプリケーションに対する安全機能を表現する場合、危険箇所という言葉は、その特定の危険に置き換えます。危険箇所と危険による結果を混同しないようにします。粉砕、切断、火傷は危険による結果です。危険箇所の例には、モータ、ラム、ナイフ、トーチ、ポンプ、レーザ、ロボット、エンドエフェクタ、ソレノイド、バルブ、その他のタイプのアクチュエータ、または重力に関連する機械的な危険箇所が含まれます。

マシンの安全関連制御システム

安全システムについて説明する場合、「安全機能に次の要求を出す時または次の要求の前に」という言い回しが使われます。安全機能に対する要求とは何でしょうか。安全機能に対する要求の例としては、インターロックガードを開く、ライトカーテンを遮る、セーフティマットを踏む、または非常停止ボタンを押すなどがあります。オペレータは、危険箇所を停止するか、またはすでに停止している場合は、停止した状態を保持するように要求します。

マシンの制御システムの安全関連部分が、安全機能を実行します。例えば、安全機能は1つの装置、例えばガードだけでは実行されません。ガードのインターロックがロジックデバイスにコマンドを送り、それによってアクチュエータが停止します。安全機能はコマンドで起動されて、実行後に終了します。

安全システムは、マシンのリスクに釣り合う安全度水準に設計する必要があります。リスクが高くなれば、安全機能の性能を保証するためにより高レベルの安全度水準が必要になります。機械安全システムはその設計意図と安全機能の性能確保能力によって分類できます。

制御システムの機能安全

__重要__：ここでは、比較的新しい規格および要件について検討します。これらの規格の一部については、起草グループが現在も作業を続けています。特に、明確化と一部の規格の結合について検討中です。したがって、この後のページに記載されている情報の一部は変更される可能性もあります。最新の情報については、ロックウェル・オートメーションの安全システムとコンポーネントのWebサイトをご覧ください：http://www.ab.com/safety

機能安全とは何か?

機能安全とは、入力に応えてプロセスまたは装置が正常に機能していることに依存する全体的な安全性の一部です。IEC TR 61508-0に、機能安全の意味を理解しやすくする例を提供しています。「例えば、過熱防止装置は機能安全の例です。これは、電気モータの巻線内の温度センサを使用して、モータが過熱する前にモータの電源を遮断します。ただし、高温に耐えるための専用断熱材は機能安全の例ではありません(それでもこれは安全装置のひとつで、まったく同じ危険から保護することができます)。」他の例として、ハードガードとインターロックガードを比較します。ハードガードは、インターロックドアと同様に危険箇所へのアクセスを防止できますが、機能安全とは認められません。インターロックドアは、機能安全のひとつです。ガードが開いているときは、インターロックは、安全状態を実現するシステムへの入力として機能します。同様に、個人用保護具(PPE)は、個人の安全性を高めるための保護手段として使用されます。PPEは、機能安全とは認められません。

機能安全という言葉は、IEC 61508:1998で紹介されました。それ以降、この言葉は時折プログラム可能な安全システムにのみ結びつけられてきましたが、これは誤解です。機能安全は、安全システムを築くために使用される幅広い範囲の装置が対象となります。例えば、インターロック、ライトカーテン、セーフティリレー、セーフティPLC、セーフティコントローラ、および安全ドライブなどの機器は相互接続されて安全システムを構成し、特定の安全関連機能を実行します。これが機能安全です。したがって、電気制御システムの機能安全は、機械の可動部に起因する危険の制御と大いに関連性があります。

機能安全を達成するためには、以下の2つタイプの要件が必要になります。

- 安全機能
- 安全整合性

機能安全の要件を開発するためには、リスクアセスメントが重要な役割を果たします。タスクと危険を分析することで、安全のための機能の要件(例えば、安全機能)を知ることができます。リスクを定量化することで、安全整合性の要件(例えば、安全度水準または安全遂行レベル)を求めることができます。

マシンに関する最も重要な制御システムの機能安全規格は、以下の4つです。

1. **IEC/EN 61508**「電気、電子およびプログラマブル電子制御システムの機能安全」
   この規格には、複雑な電子およびプログラマブルシステムおよびサブシステムの設計に適用可能な要件および対策が含まれています。この規格は一般的なので、機械部門だけに限定されません。

2. **IEC/EN 62061**「機械類の安全性 - 安全関連の電気/電子/プログラマブル電子制御システムの機能安全」
   この規格は、IEC/EN 61508の機械専用の実施です。あらゆるタイプの機械安全関連電気制御システムのシステムレベルの設計、および複雑でないサブシステムまたは装置の設計に適用される要件を明記しています。複雑なまたはプログラム可能なサブシステムにはIEC/EN 61508の安全性が要求されます。

3. **EN ISO 13849-1:2008**「機械類の安全性- 制御システムの安全関連部分」
   この規格は、以前のEN 954-1のカテゴリを使用して機能安全の変換経路を示すことを目的としています。

4. **IEC 61511**「機能安全 – プロセス産業分野の安全計装システム」
   この規格は、IEC/EN 61508のプロセス分野固有の実施です。

機能安全規格は、従来のISO 13849-1:1999 (EN 954-1:1996)の「制御信頼性」や「カテゴリ」体系など、よく知られている既存の要件から重大な前進を見せています。

カテゴリが完全にが完全になくなるわけではありません。現在のENISO 13849-1にも機能安全の概念が採用されており、新しい用語や要件が導入されています。この規格は、旧版のEN 954-1 (ISO 13849-1:1999)に大幅な追加と変更を行なったもので、大きな違いがあります。ここでは、現行のバージョンをEN ISO 13849-1と呼びます(EN ISO 13849-1:2008にもISO 13849-1:2006と同じ文章がある)。

IEC/EN 62061およびEN ISO 13849-1:2008

IEC/EN 62061およびEN ISO 13849-1は、どちらも安全関連電気制御システムを対象としています。最終的に、これらを結合させて同じ専門用語を使用する2部構成の1つの規格にすることが予定されています。どちらの規格も同じ結果をもたらしますが、使用する方法は異なります。これらは、ユーザがそれぞれの状況に最適な方を選択できるオプションを提供します。どちらの規格を使用するかは、ユーザが選択できます。ユーザはいずれかの規格を使用するか選択して、欧州の機械指令の元で両方を統合します。

両方の規格の出力は、安全性能または整合性のレベルは同等です。各規格は、対象とするユーザに合わせて異なる方法を採用しています。

IEC/EN 62061の方法は、以前の慣例に従わないシステムアーキテクチャで実施されている複雑な安全機能に対応することを目的としています。ISO13849-1:2006の方法は、従来のシステムアーキテクチャによって実施されているより旧式の安全機能のために、より直接的で複雑でない手段を提供することを目的としています。

この2つの規格の重要な違いは、多種多様なテクノロジの適用範囲です。IEC/EN 62061は、電気システムに制限されます。ISO/EN 13849-1は、空圧、油圧、機械、および電気システムに適用できます。

IEC/EN 62061およびEN ISO 13849-1での合同技術報告書

両方の規格のユーザを支援するためにIECとISO内で合同レポートが準備されました。

これは2つの規格間の関係を説明し、またシステムおよびサブシステムレベルで、EN ISO 13849-1のPL(安全遂行レベル)とIEC.EN 62061のSIL(安全度水準)との間でどのような同等性を導けるのかを説明しています。

両方の規格に同等の結果があることを示すために、レポートでは、両規格の手法に従って計算されたサンプルの安全システムを示しています。このレポートでは、異なる解釈を前提とする多くの問題についても明らかにしています。おそらく、最も重要な問題の1つが、フォルト排除の観点です。

一般的に、PLeが安全関連制御システムによって安全機能を実装するために必要な場合、このレベルのパフォーマンスを達成するためにフォルト排除のみに頼ることは普通ではありません。これは、使用されるテクノロジおよび対象となる動作環境によって左右されます。したがって、設計者がPL要件を増すためには、フォルト排除の使用についてさらに注意を払う必要があります。

一般的に、フォルト排除の使用は、安全関連制御システムの設計でPLeに到達するために、電気機械式の位置スイッチや手動作動スイッチ(非常停止装置など)の機械的観点には適用されません。特定の機械的なフォルト状態(磨耗/腐食、破断など)に適用可能なこれらのフォルト排除は、ISO 13849-2の表A.4で記載されています。

例えば、PLeを達成する必要のあるドア・インターロック・システムは、このレベルのパフォーマンスに到達するために最小フォルトトレランス1 (つまり2つの従来型の機械式位置スイッチ)を組み込む必要があります。というのも、破損したスイッチアクチュエータなどのフォルトを排除するためにこれが妥当だとは通常認められないためです。ただし、関連規格に従って設計された制御パネル内の配線の短絡などのフォルトを排除するために許容することができます。

SILおよびIEC/EN 62061

IEC/EN 62061では、リスク低減の度合いとそのリスクを低減する制御システムの能力をSIL (安全度水準)という言葉で説明しています。機械部門では、3段階のSILが使用され、SIL 1が最低でSIL 3が最高水準です。

SILという用語は、石油化学、発電、鉄道などの他の産業分野でも同じ方法で適用されるため、マシンがこのような分野で使用されているときにIEC/EN 62061は非常に有用です。プロセス産業などの他の部門では、より重大なリスクが発生する可能性があるので、IEC 61508およびプロセス部門専用の規格IEC 61511にはSIL 4も含まれます。

SILは安全機能に適用されます。安全機能を実行するシステムを構成しているサブシステムは、適切なSIL機能を備えている必要があります。これは、通常、SIL付与限界(SIL CL)と呼ばれます。適切に適用する前に、IEC/EN 62061の完全で詳細な学習が必要になります。規格の最も一般に適用される要件の一部をこのカタログの後半にまとめて説明します。

PLおよびEN ISO 13849-1:2008

EN ISO 13849-1:2008は、SILという用語は使用しません。そのかわりにPL (安全遂行レベル)という言葉を使用します。多くの点で、PLはSILと関係しています。5段階の安全遂行レベルがあり、Plaが最低レベルで、Pleが最高レベルです。

PLとSILの比較

以下の表に、あまり複雑でない電気機械テクノロジで実現された典型的な回路構造に適用される場合の、PLとSILのおおよその関係を示します。

PL (安全遂行レベル)	PFH_D (単位時間当たりの危険側故障発生確率)	SIL (安全度水準)
a	10^{-5}以上10^{-4}未満	なし
b	3 x 10^{-6} 以上10^{-5}未満	1
c	10^{-6}以上3 x 10^{-6}未満	1
d	10^{-7}以上10^{-6}未満	2
e	10^{-8}以上10^{-7}未満	3

PLとSILのおおよその対応

重要：*上に示す表は、一般的なガイドラインです。変換のために使用しないでください。変換する場合は、規格の全要件を考慮する必要があります。*

EN ISO 13849およびSISTEMAに従うシステム設計

適切に使用する前に、EN ISO 13849-1:2008の完全で詳細な学習が必要になります。以下に概要を示します。

この規格は、一部のソフトウェアの観点を含む制御システムの安全関連部分の設計と統合に要件を示しています。規格は安全関連システムに適用しますが、システムのコンポーネント部分にも適用できます。

SISTEMAソフトウェアPL計算ツール

SISTEMAは、EN ISO 13849-1の実装に使用されるソフトウェアツールです。このツールを使用すると、規格の実装を大幅に簡略化できます。

SISTEMAは、"Safety Integrity Software Tool for Evaluation of Machine Applications" (マシンアプリケーションの評価用安全保全ソフトウェアツール)の略です。これはドイツのBGIAによって開発された無料のツールです。これには、後述するさまざまなタイプの機能安全データの入力が必要です。

データは手動で入力するか、または製造メーカのSISTEMAのデータライブラリを使用して自動的に入力できます。

ロックウェル・オートメーションのSISTEMAデータライブラリは、SISTEMAのダウンロードサイトのリンクからダウンロード可能です：
www.discoverrockwellautomation.com/safety

EN ISO 13849-1の概要

この規格は広く適用可能で、電気式、油圧、空気圧、機械式などすべての技術に適用できます。ISO 13849-1は複雑なシステムに適用できますが、複雑なソフトウェア内蔵システの場合はIEC 62061およびIEC 61508も参照する必要があります。

旧版のEN 954-1と新版のEN ISO 13849-1の間の基本的な違いについて見てみます。旧規格の出力は、カテゴリ[B, 1, 2, 3または4]で、新規格の出力は、安全遂行レベル[PL a, b, c, dまたはe]です。カテゴリの概念は残りますが、システム内でPLを要求する上で満たすべき追加要件があります。

この要件は、次のような基本フォームで一覧表示されています。

- システムのアーキテクチャ。基本的に、これは、カテゴリとして使用されるようにしたものを取得します。
- システムの構成部品に信頼性データが必要です。
- システムの自己診断率[DC]が必要です。これは事実上システムの故障モニタの量を表します。
- 共通原因故障に対する保護
- 系統的故障に対する保護
- 必要に応じて、ソフトウェア固有の要件

この後、各要素について詳細に見ていきますが、それを行なう前に、規格全体の基本的な目的および原則について検討してみます。この段階で新たに習得することがあることは確かですが、規格が達成しようとしている目的とその理由を把握しておいた方が規格の詳細について理解しやすくなります。

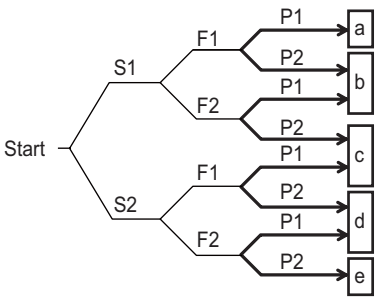
まず、なぜ新しい規格が必要になったのでしょうか。機械の安全システムで使用されている技術は、過去10年間の間に大幅に進歩し、変化しました。比較的最近まで、安全システムは、予知や予測が非常に容易な故障モードのある「シンプルな」機器に依存していました。しかし最近では、より複雑な電気式のプログラミング可能なデバイスが安全システムで使用されるようになってきました。これは、費用、柔軟性、および互換性について大きな利点がありますが、既存の規格では対応しきれなくなったことも意味します。安全システムが十分に良好であるかどうかを把握するために、安全システムをより詳細に理解する必要があります。これが、新しい規格により多くの情報が求められている理由です。安全システムがより「ブラックボックス」的な手法を採用するにつれて、規格に適合していることをより重視するようになってきました。したがって、これらの規格には、適切に技術を調べることのできる能力が必要になります。これを満たすために、信頼性、障害検出、アーキテクチャ上の整合性、およびシステム上の完全性に関する基本的な要素を取り扱う必要があります。これが、EN ISO 13849-1の目的です。

この規格全体を通して論理的に理解するために、2つの基本的に異なるユーザタイプを考慮する必要があり、これは安全関連サブシステムの設計者と、完全関連システムの設計者です。一般的に、サブシステムの設計者(通常は安全コンポーネントの製造メーカ)は、よりレベルの高い複雑な作業を求められます。システム設計者は、サブシステムがシステムに対して十分な整合性を保っていることを保証できるように、必要なデータを提供する必要があります。これは、通常、一部のテスト、分析、計算で必要です。その結果は、規格によって要求されるデータの形式で表されます。

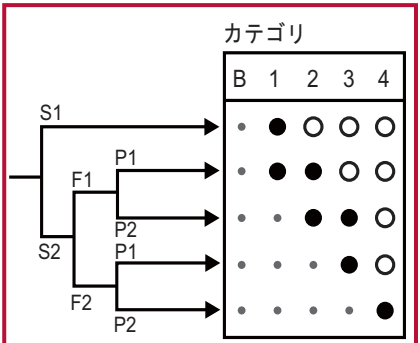
システム設計者[通常は、マシンの設計者またはインテクグレータ]は、サブシステムデータを使用して、比較的簡単な計算を実行して、システムの全体的な安全遂行レベル(PL)を評価します。

PLrは、安全機能で必要な安全遂行レベルを示すのに使用されます。この規格では、PLrを判断するためのリスクのグラフが用意されていて、傷害の程度、危険にさらされる頻度、および回避の可能性についてのアプリケーション要素を入力します。

EN ISO 13849-1:2008に従うシステム設計



EN ISO 13849-1の付録Aからのリスクのグラフ



EN 945-1の付録Bからのリスクのグラフ

出力がPLrになります。旧版のEN 954-1のユーザはこの手法に慣れ親しんでいますが、S1線が分岐していて、旧リスクグラフでは分岐していないことに注意してください。つまり、より低いリスクレベルでも安全対策の完全性について再考しなければならない可能性があるということです。

ただし、非常に重要な部分に触れる必要があります。この規格からは、システムに求められているレベルやそのレベルを判断する方法がわかりますが、実行すべきことについてはわかりません。どのような安全機能にするのかを決める必要があります。安全機能が作業にとって適正なものになる必要があるのは明らかですが、これをどの程度保証すればよいのでしょうか。この規格はどのように役立つのでしょうか?

必要な機能は、実際の用途で一般的な特性を考慮することでのみ決定できるということを理解することが重要です。これは安全概念の設計段階と呼ぶことができます。この規格は特定の用途の全特性について把握しているわけではないので、この規格ですべてを網羅することはできません。また、機械を製造しているものの、使用される正確な条件を必ずしも理解していないマシンビルダーにもしばしば適用されます。

この規格は、一般的に使用される多くの安全機能(安全装置による安全関連停止機能、消音機能、開始/再開機能など)についてリストアップし、一般的に関連のある要件を定めることで便宜を図っています。この段階では、他の規格(EN ISO 12100：基本設計原則、EN ISO 14121：リスクアセスメントなど)を使用することを強く推奨します。また、特定の機械に対するソリューションを提供する機械固有の規格も幅広く用意されています。欧州のEN規格内では、これらはCタイプ規格と呼ばれており、その一部はISO規格とまったく同一です。

安全概念の設計段階は、機械の種類と使用されている用途と環境の特性にも依存していることが理解できると思います。機械の製造メーカは、安全の概念を設計できるようにするためにこれらの要素を予想しておく必要があります。意図した(つまり予測される)使用条件を、ユーザーズマニュアルに記載しておく必要があります。機械のユーザは、それが実際の使用条件に合っていることをチェックする必要があります。

次に、安全機能について説明します。規格の付録Aには、この機能を実装するために使用される制御システムの安全関連部(SRP/CS)の必要な安全遂行レベル(PLr)が定められています。ここでシステムの設計が必要になり、この設計がPLrに適合していることを確認します。

使用する規格(EN ISO 13849-1またはEN/IEC 62061)を決定するための重要な要素の1つが、安全機能の複雑性です。ほとんどの場合、機械類に対して、安全機能は比較的シンプルで、EN ISO 13849-1は最適なルートとなります。信頼性データ、自己診断率(DC)、システムアーキテクチャ(カテゴリ)、共通原因故障、および(関係のある場合)ソフトウェアの要件がPLの評価に使用されます。

これは、概要を把握するための簡略化された説明です。この規格の本文に指定されたすべての条項を適用する必要があることを理解することが重要です。しかし、これに役立つツールもあります。SISTEMAソフトウェアツールを使用すると、文書化および計算の部分に役立ちます。また、技術ファイルも生成してくれます。

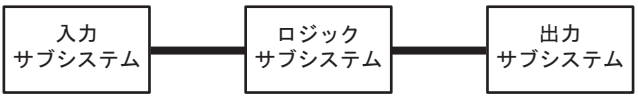
SISTEMA には、本カタログの発行時点で英語版とドイツ語版があります。他の言語については、近々リリースされる予定です。SISTEMAの開発元であるBGIAは、ドイツに拠点を置く、信頼性の高い研究およびテスト機関です。主に、ドイツにおける法定災害の保険や予防の分野で、安全性に関する科学的および技術的問題の解決に携わっています。この機関は、20ヶ国以上の労働安全衛生機関と協力して作業に当たっています。BGIAの専門家は、BGの担当者と共に、EN ISO 13849-1およびIEC/EN 62061の草案作成に深く関与してきました。

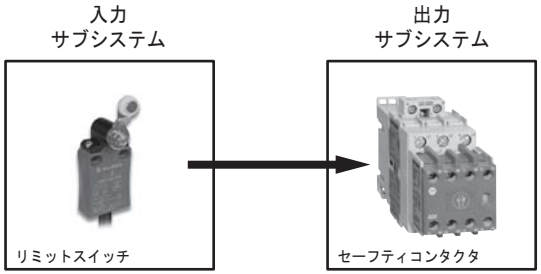
SISTEMAに関するロックウェル・オートメーションの安全コンポーネントデータの「ライブラリ」は、以下のWebサイトをご覧ください：
www.discoverrockwellautomation.com/safety

いずれのPLの計算方法が行なわれていても、正しい根拠から開始することが重要です。この規格と同じ方法でシステムを検討することが必要になるため、まずそこからはじめてください。

システム構造

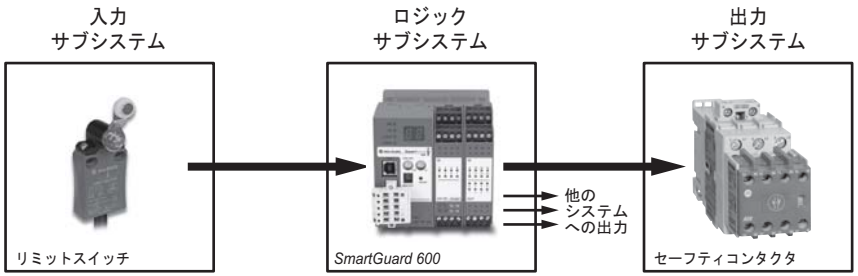
あらゆるシステムは、基本システムコンポーネント、つまり「サブシステム」に分割することができます。各サブシステムにはそれぞれ独自の機能があります。ほとんどのシステムは、3つの基本機能(入力、論理的解決、作動)に分割することができます(一部の単純なシステムには論理解決機能のないものもあります)。これらの機能を実装しているコンポーネントグループがサブシステムです。





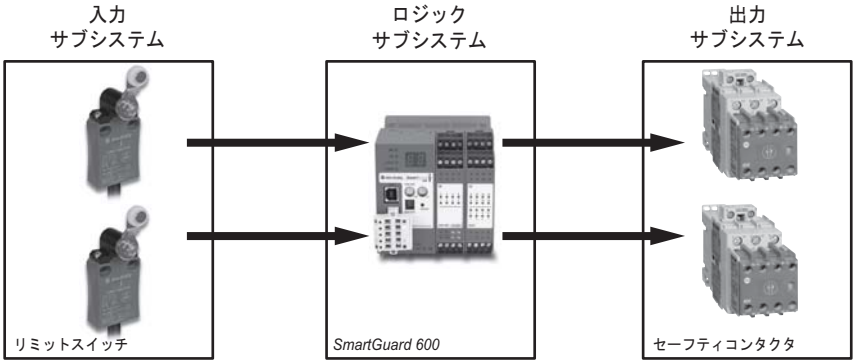
インターロックスイッチおよびコンタクタ

上図に、シンプルなシングルチャネルの電気的なシステム例を示します。これは、入力と出力サブシステムだけで構成されています。



インターロックスイッチ、セーフティコントローラ、およびコンタクタ

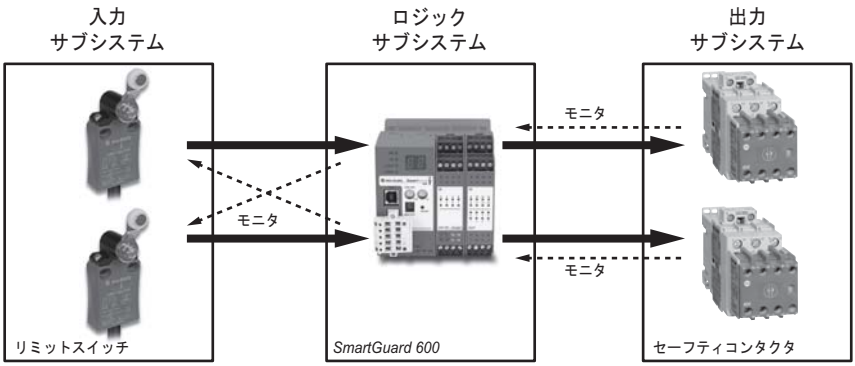
上図のシステムはもう少し複雑で、いくつかの論理演算が必要になります。セーフティコントローラ自体は内部にフォルトトレランス(つまりデュアルチャネル)を備えていますが、システム全体は、単一リミットスイッチおよび単一コンタクタであるため、シングルチャネル状態のままです。



デュアルチャネル安全システム

前の図の基本アーキテクチャを採用した場合、考慮すべきものが他にもいくつかあります。まず、システムに「チャネル」がいくつあるでしょうか。サブシステムの1つが故障すると、シングル・チャネル・システムは機能しません。2チャネル(いわゆる冗長)システムは、2つのチャネルが故障しないと、システム全体は故障しません。チャネルが2つあるため、単一フォルト(故障)に対して耐性があり、動作し続けることができます。上図に、2チャネルのシステムを示します。

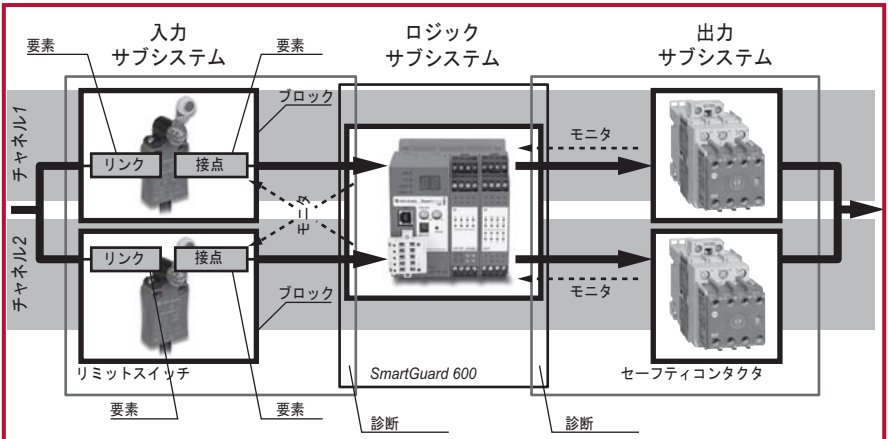
2つのチャネルのシステムが1つのチャネルのシステムよりも故障する確率が低いのは明らかですが、フォルト(故障)検出の診断手順が含まれている場合、(安全機能の観点で)さらに信頼性の高いものにすることができます。もちろん、フォルトを検知した場合に、これに対応してシステムを安全な状態にする必要があります。以下の図は、モニタ技法を通じて実現される診断手順が含まれていることを示しています。



デュアルチャネル安全システムでの診断

必ずではありませんが、以下の図に示すように、すべてに2つのチャネルがあるサブシステムでシステムが構成されていることが一般的です。したがって、この場合各サブシステムに2つの「サブチャネル」があることがわかります。この規格ではこれらを「ブロック」と表現しています。2チャネルのサブシステムには2つのブロックがあり、シングル・チャネル・サブシステムには1つのブロックがあります。一部のシステムでは、デュアル・チャネル・ブロックとシングル・チャネル・ブロックを組み合わせることができます。

このシステムをより深く検討したい場合、ブロックのコンポーネント部品に着目する必要があります。SISTEMAツールは、このようなコンポーネント部品について「エレメント」という用語を使用しています。以下の図に、SISTEMA用語を使用してシステムを示したものを示します。



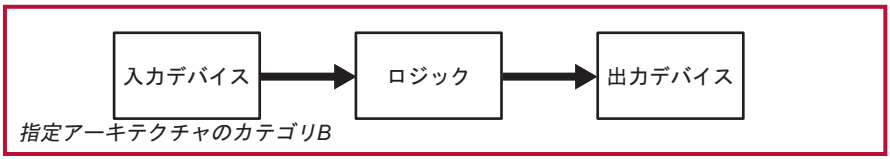
デュアルチャネル安全システムで、診断付きで分割されたシステム

リミットスイッチのサブシステムは、エレメントレベルまで細分化されていることがわかります。出力コンタクタサブシステムは、ブロックレベルまで細分化されていて、論理サブシステムはまったく細分化されていません。リミットスイッチとコンタクタのモニタ機能は、ロジックコントローラで実行されます。したがって、リミットスイッチとコンタクタサブシステムを表す四角は、論理サブシステムを表す四角と一部重なり合っています。

システム細分化の原則は、EN ISO 13849-1で指定された用語と、SISTEMAツールの基本システム構造原則で認識できます。ただし、微妙な違いもあることに注意が必要です。この規格は手法に制限がありませんが、PLを評価する簡略化された手法では、通常第1ステップで、システム構造をチャネルと各チャネル内のブロックに分解します。SISTEMAでは、最初にシステムをサブシステムに分割します。この規格ではサブシステムの概念を明確に記述していませんが、SISTEMAでは、より理解可能で直感的な手法でサブシステムの概念を使用しています。もちろん最終的な計算には影響しません。SISTEMAとこの規格ではいずれも同じ原則と式を使用しています。興味深いことに、サブシステム手法はEN/IEC 62061でも使用されています。

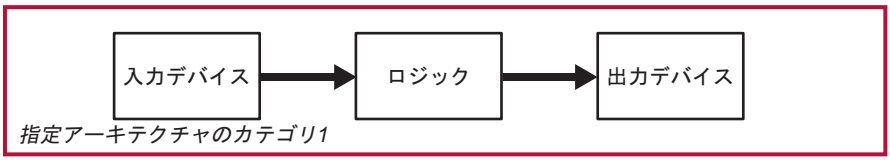
例として使用しているシステムは、規格で明示されているシステムアーキテクチャの5つの基本タイプの1つにすぎません。カテゴリシステムをよく理解しているユーザであれば、お気づきのようにこの例はカテゴリ3または4に相当します。

この規格では、従来のEN 954-1カテゴリを、指定システムアーキテクチャの5つの基本タイプとして使用しています。これらは、指定アーキテクチャカテゴリと呼ばれます。カテゴリの要件は、EN 954-1で定められていたカテゴリの要件と、完全ではないもののほぼ同一です。指定アーキテクチャカテゴリは、以下の図で表されます。各カテゴリはシステム全体にもサブシステムにも適用できることに注意してください。これらの図は、そのまま物理構造としてとらえるべきではなく、概念的な要件をグラフィカルに表したものです。



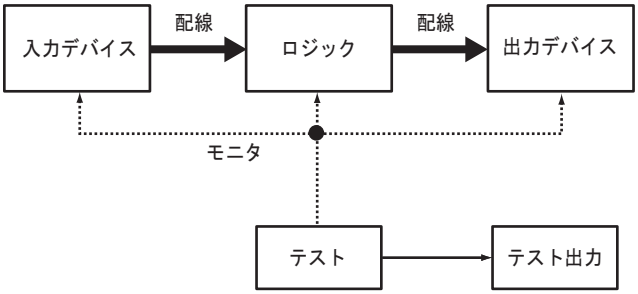
指定アーキテクチャのカテゴリB

指定アーキテクチャのカテゴリBは、基本的な安全原理(EN ISO 13849-2の付録を参照)を使用する必要があります。単一フォルトの発生時には、システムやサブシステムが故障する可能性があります。完全な要件については、EN ISO 13849-1を参照してください。



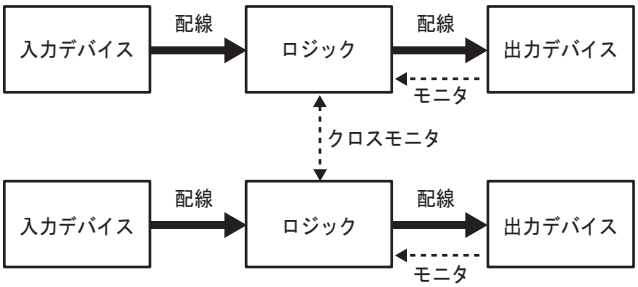
指定アーキテクチャのカテゴリ1

指定アーキテクチャのカテゴリ1はカテゴリBと同じ構造で、単一フォルトの発生時に全体が故障する可能性があります。ただし、十分テストされた安全原則(EN ISO 13849-2の付録を参照)を使用する必要もあるので、フォルト派生の可能性はカテゴリBよりも低くなります。完全な要件については、EN ISO 13849-1を参照してください。



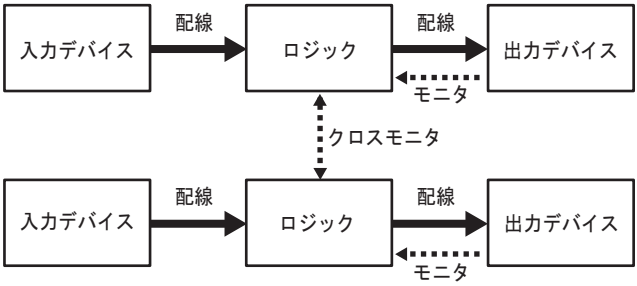
指定アーキテクチャのカテゴリ2

指定アーキテクチャのカテゴリ2は、基本的な安全原理(EN ISO 13849-2の付録を参照)を使用する必要があります。さらに、システムやサブシステムの機能テストによって診断モニタを行なう必要もあります。これは始動時に実施し、その後は安全機能への各要求に対して、少なくとも100回のテストに相当する頻度で定期的に実施する必要があります。このテスト頻度は、旧版のEN 954-1で指定された追加要件です。機能テストの間に単一フォルトが発生すると、システムやサブシステムにフォルトが発生する可能性がありますが、その可能性は、通常カテゴリ1よりも低くなっています。完全な要件については、EN ISO 13849-1を参照してください。



指定アーキテクチャのカテゴリ3

指定アーキテクチャのカテゴリ3は、基本的な安全原理(EN ISO 13849-2の付録を参照)を使用する必要があります。さらに、単一フォルトの発生時にシステムやサブシステムにフォルトが発生してはならないという要件もあります。つまり、システムは、安全機能に関してシングル･フォルト･トレランス設計になっている必要があります。この要件を満たす上で最も一般的な方法は、上図に示すデュアル・チャネル・アーキテクチャを採用することです。このほか、可能な限り単一フォルトを検出することも求められます。この要件は、EN 954-1のカテゴリ3に定められている従来の要件と同一です。この場合に、「可能な限り」というフレーズの意味は少々あいまいでした。これでは、カテゴリ3には、冗長性を備えているもののフォルト検出はできないシステム(しばしば「愚かな冗長性」と的確に描写されています)から、単一フォルトをすべての検出できる冗長システムまでが含まれていることになります。EN ISO 13849-1では、自己診断率(DC)の品質を評価するための要件によってこの問題を解決しています。システムの信頼性(MTTFd)が増加すれば、必要なDCは減少します。ただし、カテゴリ3アーキテクチャでは、DCが60%以上であることが必要です。



指定アーキテクチャのカテゴリ4

指定アーキテクチャのカテゴリ4は、基本的な安全原理(EN ISO 13849-2の付録を参照)を使用する必要があります。カテゴリ3の要件の図と似ていますが、より多くのモニタ、つまり高い自己診断率が求められています。これは、モニタ機能を示す点線が太くなっていることで表現されています。カテゴリ3と4の基本的に違いは、カテゴリ3ではほとんどのフォルトを検出する必要があり、カテゴリ4ではすべての単一フォルトを検出する必要があることです。DCは99%以上であることが求められています。フォルトが累積されて危険故障を発生することも許されません。

信頼性データ

EN ISO 13849-1は、制御システムの安全関連部によって達成されるPLの計算の一部として、定量的な信頼性データを使用使用します。これは、EN 954-1と大きく異なる点です。最初に浮かぶのは、「データはどこから取得するのか」という疑問です。信頼性について定評のあるハンドブックのデータを使用することもできますが、この規格では、推奨する情報源は製造メーカであることを明確にしています。このためロックウェル・オートメーションでは、関連情報をSISTEMA用のデータライブラリという形で利用できるようにしています。いずれは、他の形式でもデータを公開する予定です。先に進む前に、必要なデータの種類について検討し、そのようなデータを生成する方法について理解する必要があります。

この規格(およびSISTEMA)でのPLの評価の一環として必要になる最終的なデータの種類は、PFH (単位時間当たりの危険側故障確率)です。これは、IEC/EN 62061で使用されているPFH_Dという略語で表現されているデータと同じものです。

PL (安全遂行レベル)	PFH_D (単位時間当たりの平均危険側故障確率)	SIL (安全度水準)
a	10^{-5}以上<10^{-4}未満	なし
b	3 x 10^{-6}以上<10^{-5}未満	1
c	10^{-6}以上<3 x 10^{-6}未満	1
d	10^{-7}以上<10^{-6}未満	2
e	10^{-8}以上<10^{-7}未満	3

上表に、PFHとPLとSILの関係を示します。一部のサブシステムについて、PFHは製造メーカから取得できます。この場合は計算が簡単になります。製造メーカは通常、PFHを提供するためにサブシステムに対して比較的複雑な計算やテストを実施しなければなりません。PFHが提供されない場合、EN ISO13849-1では、シングルチャネルの平均MTTFd (平均危険故障時間)に基づく簡単な代替方法が提供されています。この代替手法では、この規格で定められている手法と式を使用して、システムやサブシステムのPL(およびPFH)を計算できます。SISTEMAを使用することでさらに簡単に計算できます。

注：(診断付きまたはなしの)デュアル・チャネル･システムの場合、1/ PFH_Dを使用してEN ISO 13849-1の求めるMTTFdを決定することは間違っていることを理解しておくことが重要です。この規格では、シングルチャネルのMTTFdが必要とされています。2チャネルサブシステムの両チャネルの組み合わせとは、MTTFdの値は大きく異なります。2チャネルサブシステムのPFH_Dがわかっている場合、それをSISTEMAに直接入力することができます。

シングルチャネルのMTTFd

MTTFdは、安全機能の故障につながる可能性のあるフォルト(故障)が発生するまでの平均時間を表すもので、年数で表されます。シングルチャネルにおける「ブロック」のMTTFdの平均値であり、システムにもサブシステムにも適用できます。この規格では、以下の式が定められており、この式を使用して、シングルチャネルまたはサブシステムで使用されている各エレメントのすべてのMTTFdの平均を計算します。

この段階で、SISTEMAの値が明らかになります。ユーザは、こうした作業をソフトウェアで実行できるので、表の参照や式の計算に時間を使う必要がなくなります。最終結果は、複数ページのレポートの形式で印刷できます。

$$\frac{1}{MTTF_d} = \sum_{i=1}^{\tilde{N}} \frac{1}{MTTF_{di}} = \sum_{j=1}^{\tilde{N}} \frac{nj}{MTTF_{dj}} \quad \text{(EN ISO 13849-1からの式D1)}$$

ほとんどのデュアル・チャネル・システムでは、両方のチャネルが同一なので、式の結果はいずれのチャネルにも当てはまります。

この規格では、システムやサブシステムのチャネルが異なる場合に対応した式も定められています。

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}} \right]$$

これは要するに、2つの平均値を平均したものです。簡略化を目的として、最悪のチャネル値のみを使用することもできます。

この規格では、MTTFdを以下のように3つの範囲にグループ分けしています。

チャネルごとのMTTFdの意味	チャネルごとのMTTFdの範囲
低	3年≦MTTFd < 10年
中	10年≦MTTFd < 30年
高	30年≦MTTFd < 100年

$MTTF_d$のレベル

EN ISO 13849-1では、導き出された実際の値がより長いものであっても、シングルチャネルのMTTFdの使用を最大100年に制限していることに注意してください。

後で説明するように、このMTTFd平均値の範囲を指定アーキテクチャカテゴリおよび自己診断率(DC)と組み合わせると、予備的なPL評価値が得られます。ここで「予備的」という用語を使用しているのは、システムの整合性や共通原因故障への対策など他の要件も必要に応じて満たさなければならないからです。

データ評価の手法

製造メーカがPFH$_D$またはMTTFdの形式でデータを評価する方法について、もう少し詳しく検討する必要があります。製造メーカのデータを扱う際には、この点を理解しておくことが重要です。コンポーネントは、3つの基本タイプにグループ分けされています。

- 機械的(電気機械式、空圧、および油圧など)
- 電子的(ソリッドステート)
- ソフトウェア

これらの3種類のテクノロジで発生する一般的な故障のメカニズムには、根本的な違いがあります。基本的には次のように要約することができます。

機械的なテクノロジ:

故障は固有の信頼性および使用量に比例します。使用量が増加するほど、コンポーネント部品のいずれかが品質低下および故障する可能性が高まります。これだけが故障の理由とはなりませんが、運転時間/サイクルが制限されている場合を除いて、主要な原因となります。切換えサイクル10秒に1回のコンタクタの方が、1日に1回しか動作しない同じコンタクタよりも信頼性がある状態で動作する期間がはるかに短いのは自明のことです。一般的に物理的テクノロジ装置は、それぞれ固有の用途向けに設計されたコンポーネントで構成されています。各コンポーネントは、シェーピング、モーディング、キャスティング、マシニングなどによって製造されます。また、リンク、スプリング、磁石、電気巻線などを組み合わせて、メカニズムを形成しています。一般に、コンポーネント部品は他の用途での使用歴がないので、既存の信頼性データを見つけられません。PFH$_D$またはMTTFdの評価は、通常テストに基づいて行なわれます。EN/IEC 62061およびEN ISO 13849-1のいずれも、B10dテストと呼ばれるテストプロセスを推奨しています。

B10dテストでは、では、複数(通常は10個以上)のデバイスサンプルを適切な典型的条件のもとでテストされます。サンプルの10%が危険な状態に陥るまでの動作サイクルの平均値がB10d値と呼ばれるものです。実際には、サンプルがすべて安全な状態になることもよくありますが、その場合B10d (危険)値はB10 (安全)値の2倍とすることができるとこの規格には明記されています。

電子的なテクノロジ:

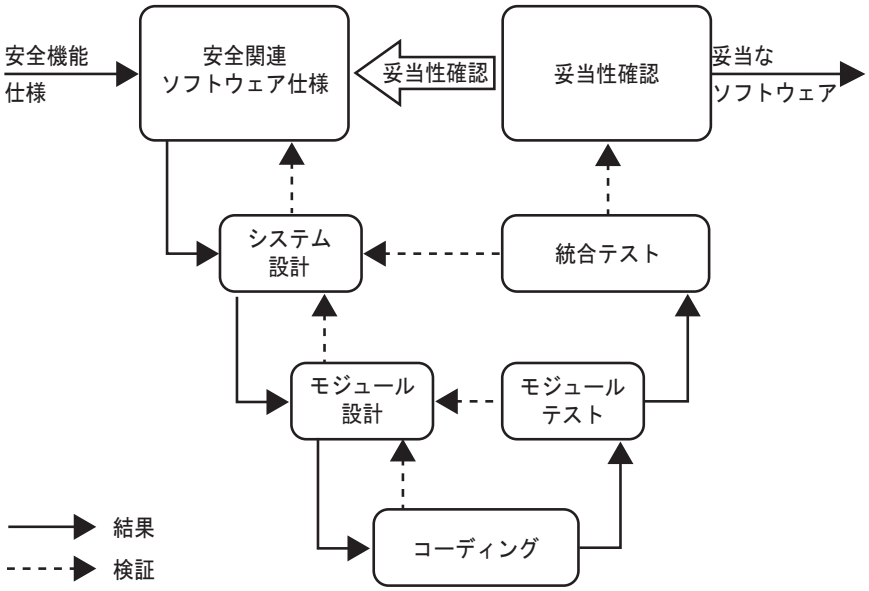
物理的な磨耗が生じる可動部がありません。特定の電気的特性や温度特性などに当てはまる動作環境では、電子回路の主な故障は、構成コンポーネントの信頼性(または信頼性のなさ)に比例します。個別のコンポーネントの故障原因には、製造時の欠陥、過度な電力サージ、機械的な接続の問題などさまざまなものがあります。一般的に、電子コンポーネントの故障は、分析による予測が困難で、ランダムに発生する傾向があるようです。したがって、テスト環境下で電子機器をテストしても、典型的な長期的故障パターンは必ずしも明らかになりませ。

電子機器の信頼性を評価するには、分析と計算を使用するのが一般的です。信頼性データのハンドブックには、個別のコンポーネントの正確なデータが掲載されています。どのコンポーネント故障モードが危険であるかは、分析によって判断できます。平均してコンポーネント故障モードの50%が安全で、50%が危険であるというのが許容可能で一般的です。通常これは、比較的控えめなデータになります。

IEC 61508は、デバイス(つまりサブシステム)の全体的な危険故障確率(PFHまたはPFD)の計算に使用できる式が定められています。この式はかなり複雑で、(必要に応じて)コンポーネントの信頼性、共通原因故障の可能性(ベータ係数)、自己診断率(DC)、機能テストの間隔、およびプルーフテストの間隔を考慮します。幸いなことに、この複雑な計算は通常デバイス製造メーカによって行なわれます。EN/IEC 62061とEN ISO 13849-1の両方とも、IEC 61508に対して、この方法で計算されたサブシステムを認めています。この結果として得られたPFHDは、EN ISO 13849-1の付録KまたはSISTEMA計算ツールのいずれかで直接使用できます。

ソフトウェア:

ソフトウェアの故障は本質的に系統的な性質のものです。あらゆる故障は、そのソフトウェアがどのように考案、記述、またはコンパイルされたかに起因します。したがって、すべての故障の原因は、ソフトウェアの使用ではなく、製造元となったシステムです。したがって、故障を抑制するには、システムを制御する必要があります。IEC 61508とEN ISO 13849-1の両方とも、そのための要件と手法が定められています。従来のVモデルを使用するという点以外は、ここでは詳細は説明する必要はありません。組込みのソフトウェアは、デバイス設計者にとって問題となります。一般的な手法としては、IEC 61508パート3で説明されている正式な手法に従って組込みソフトウェアを開発します。ユーザがインターフェイスで接続するソフトウェアであるアプリケーションコードについては、ほとんどのプログラマブル安全装置に「認定済み」ファンクションブロックやルーチンが提供されています。これを利用すると、アプリケーションコードの検証作業が簡略化されますが、完成したアプリケーションプログラムには検証が必要なことを忘れてはなりません。ブロックをリンクし、パラメータ化する方法は、目的の作業にとって適切かつ有効であることが実証されている必要があります。EN ISO 13849-1とIEC/EN 62061の両方とも、このプロセスのガイドラインが定められています。



ソフトウェア開発のためのVモデル

自己診断率(DC)

このことについては、指定アーキテクチャカテゴリ2、3および4について検討した際にすでに触れています。これらのカテゴリでは、何らかの形態の診断テストによって、安全機能が働いているかどうかを確認する必要があります。「自己診断率」(通常はDCと略記)という用語は、このようなテストの有効性を特長付けるために使用されます。DCは、危険な故障が発生する可能性のあるコンポーネントの数だけに基づいているわけではないことを理解することが重要です。全体的な危険側故障率も考慮に入れられています。「故障率」を表すのに記号λ(ラムダ)が使用されます。DCは、以下の2種類の危険側故障の発生率の関係を表します。

検出危険側故障[λdd]：安全機能の損失の原因となる(または損失につながる可能性のある)検出された故障。検出後、故障応答機能によってデバイスやシステムを安全な状態に戻します。

危険側故障[λd]：安全機能の損失の原因となる可能性がある(または損失につながる可能性のある)すべての故障。これには、検出された故障も検出されていない故障も含まれます。もちろん、本当に危険な故障は未検出危険側故障[λdu]です。

DCは、以下の式で表されます。

DC = λdd/λd (割合(%)で示す)

DCという用語の意味は、EN ISO 13849-1とEN/IEC 62061で共通しています。ただし、その導き方は異なっています。EN/IEC 62061では故障モード分析に基づいた計算の利用を提唱していますが、EN ISO 13849-1ではルックアップテーブル形式の簡略化された手法を定めています。各種の一般的な診断技法が、それぞれの使用で達成すると考えられるDCの割合(%)と共に掲載されています。一部のケースでは、依然として推理的な判断が必要なものもあります。例えば、一部の技法では、得られるDCはテストの実施頻度に比例します。この手法は不確実すぎるという意見もありますが、DCの評価は多くの異なる変動要素に依存しているので、いずれの技法を使用しても、通常結果は概算値で表すことしかできません。

また重要な点として、EN ISO 13849-1の表はBGIAが実施した広範な調査に基づいていて、実際の用途で使用されている既知の実際の診断技法で得られた結果になっています。この規格では、簡略化のために、DCを以下の4つの基本的な範囲に分けています。

60%未満 = なし
60～90% = 低
90～99% = 中
99%以上 = 高

個別の割合(%)値のかわりに範囲を使用するこの手法は、達成可能な精度の面でより現実的であると見なされます。SISTEMAツールは、この規格と同じルックアップテーブルを使用します。安全関連装置の複雑な電子機器の使用増加に伴い、DCはますます重要な要素になっています。各規格における今後の作業では、この問題の明確化がさらに検討されるようです。それまで、DCの範囲の適切な選択には工学的な判断と常識を用いるだけで十分です。

共通故障原因(CCF)

ほとんどのデュアルチャネル(つまりシングル・チャネル・トレランス)のシステムまたはサブシステムにおいて、診断の仕組みは、両方のチャネルの危険側故障が同時に発生しないという前提に基づいています。「同時に」という言葉を正確に表現すると、「同じ診断テスト間隔で」となります。診断テスト間隔が適度に短い場合(8時間未満)、2つの独立した無関係の故障がその時間内に発生する可能性はきわめて低いと仮定するのが合理的です。ただし、この規格では、故障が本当に独立した無関係のものであるかどうか慎重に検討すべきである点を明確にしています。例えば、1つのコンポーネントの故障が他のコンポーネントの故障につながることが予想できる場合、故障全体は単一フォルトであると考えられます。

また、1つのコンポーネントの故障原因となる事象が他のコンポーネントの故障原因となる可能性もあります。これは「共通原因故障」(CCF)と呼ばれます。CCFが発生する傾向の度合いは、通常ベータ(β)係数で表されます。サブシステムやシステムの設計者がCCFの可能性を認識することはきわめて重要です。さまざまな種類のCCFが存在し、それに応じて回避方法も数多く存在します。EN ISO 13849-1では、複雑すぎでも単純すぎでもない合理的な筋道に従っています。EN/IEC 62061と同様に、本質的に定性的な手法が採用されています。CCFの回避に効果的と認められている対策のリストが提供されています。

No.	CCF対策	スコア
1	隔離/分離	15
2	ダイバーシティ(多様性)	20
3	評価/アプリケーション/経験	20
4	評価/分析	5
5	能力/トレーニング	5
6	環境	35

共通故障原因(CCF)のスコアリング

システムやサブシステムを設計する際に、このリストの中から十分な数の対策を導入する必要があります。このリストを使用するだけではCCFの可能性を完全に回避することはできないという主張にも、ある程度の正当性はあるかもしれません。しかし、リストの目的を正しく考えれば明らかなように、この要件の真意は、設計者がCCFの可能性を分析して、テクノロジの種類と対象用途の特性に基づいて適切な回避策を導入できるようにすることです。リストを使用することによって、多様な故障モードや設計能力など、最も基本的で効果的な技法の一部を検討することができます。BGIA SISTEMAツールでも、この規格のCCFルックアップテーブルの導入が必要で、利便性の高い形で利用できるようにしています。

系統的故障

MTTFdや危険側故障確率の形式で定量化された安全信頼性データについてすでに検討してきましたが、これがすべてではありません。これらの用語に言及した際は、ランダムな性質と思われる故障について検討しました。実際にIEC/EN 62061では、PFH_Dの略語は、具体的にランダムなハードウェア故障の確率を指しています。しかし、設計プロセスや製造プロセスでのエラーに起因する種類の故障も存在し、「系統的障害」と総称されています。この代表的な例は、ソフトウェアコードのエラーです。付録Gには、このようなエラー(およびそれに伴う故障)を回避するための対策が定められています。これらの対策には、適切な素材および製造技法、レビュー、分析、およびコンピュータシミュレーションの利用などの対応が含まれています。動作環境では、結果を制御しなければ故障の原因となる予測可能な事象や特性も発生します。付録Gには、これを回避するための対策も定められています。例えば、電力の損失が発生することは容易に予測できます。したがって、コンポーネントの電源が切断されても、システムは安全な状態を維持できるようにする必要があります。このような対策は単に常識と思われがちで、実際にそうですが、極めて重要なことです。系統的障害の抑制や回避に対して適切な考慮を払わない場合、この規格の他のすべての要件は無意味なものとなります。これは、自動診断テストや冗長ハードウェアなど、必要なPFH_Dを達成するために、ランダムなハードウェア故障の抑制に使用されるものと同等の対策が求められる場合もあります。

フォルト排除

故障分析は安全システム用の主要な分析ツールの1つです。設計者とユーザは、フォルトが存在するときに安全システムがどのように実行されるかを理解する必要があります。分析を行なうためにさまざまな方法を使用できます。例えば、故障のツリー解析、故障モード、効果および致命度解析、イベントのツリー解析、および負荷強度検査などがあります。

分析中に、、特定のフォルトを発見できないこともあります。これは、費用を節減した自動診断テストでは検出できないためです。さらに、これらのフォルトが発生する可能性は、軽減設計、構造、およびテスト方法を使用することにより、極めて小さくすることもできます。このような状況では、さらに検討することによりフォルトを排除できる可能性もあります。フォルト排除とは、SRCSの特定の故障の確率が無視できる程度であるため、その故障の発生を排除することです。

ISO13849-1:2006では、技術的に発生しそうにないこと、一般に認められている技術的な経験、およびアプリケーションに関連する技術的要件に基づいたフォルト排除を認めています。ISO13849-2:2003では、電気、空圧、油圧、および機械式システムに関して特定のフォルトを排除するための例と正当性も示しています。フォルト排除は、正当性を詳細に示した上で、技術文書で宣言する必要があります。

特定のフォルト排除可能性を排除して安全関連制御システムを評価することは、常に可能なわけではありません。。フォルト排除については、ISO 13849-2を参照してください。

リスクのレベルが高くなると、フォルト排除の妥当性より厳しいものになります。通常、安全関連制御システムで実装される安全機能のためにPLが必要とされる場合は、このレベルの性能を達成するためにフォルト排除のみに頼ることは一般的なことではありません。これは、使用されるテクノロジと対象となる動作環境によって左右されます。そのため、設計者は、PL要件が増すにつれてフォルト排除の使用に十分な注意を払うことが必要となります。

例えば、PLeを実現するために必要なドア・インターロック・システムは、スイッチアクチュエータの破損などのフォルトを排除することが通常は妥当とは認められないため、このレベルのパフォーマンスに達成するために、最小フォルトトレランス1 (例えば、2つの従来型の機械式位置スイッチ)を組込む必要があります。ただし、関連する規格に従って設計された制御パネル内の配線の短絡などのフォルトを排除するために、これは許容することができます。

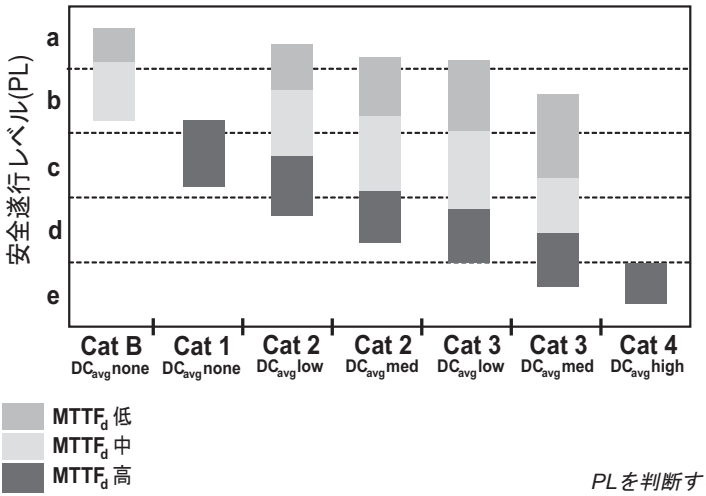
安全遂行レベル(PL)

安全遂行レベルは、制御システムの安全関連部分が安全機能を実行する能力を特定する離散レベルです。

5つの指定されたアーキテクチャのいずれかを実行して実現されたPLを評価するには、システム(またはサブシステム)に関する以下のデータが必要です。

- $MTTF_d$ (各チャネルの危険側故障発生までの平均時間)
- DC (自己診断率)
- アーキテクチャ(カテゴリ)

以下の図に、これらの要素を組み合わせてPLを判断するための方法を示します。本書の最後に記載する表に、この図の基本を使用して作成した異なるマルコフモデルの結果の表を示します。より正確な判断が必要な場合は、表を参照してください。



PLを判断するための方式

目標とするPLを達成するには、他の要素も実現する必要があります。これらの要件には、共通原因故障、系統的故障、環境条件、および活動時間に対する措置も含まれます。

システムまたはサブシステムのPFH_Dがわかっている場合は、表10.4 (規格の付録K)を使用してPLを特定できます。

サブシステム設計および組合せ

すべてのサブシステムのPLがわかっているときは、以下の表を使用して簡単にシステムに組み合わせることができます。この表の陰にある論理は明らかです。1つ目は、システムのレベルは、最も低レベルのサブシステムと同じになることです。2つ目は、サブシステムの数が多くなると、それだけ故障の発生確率も高くなることです。

PL_{low}	N_{low}	PL
a	>3	適用しない
	≦3	a
b	>2	a
	≦2	b
c	>2	b
	≦2	c
d	>3	c
	≦3	d
e	>3	d
	≦3	e

直列に組み合わせたサブシステムのPL計算

以下の図に示すシステムでは、安全遂行レベルはが最も低いのはサブシステム1と2で、両方ともPLbです。したがって、左の表を使用してb (PL_{low}列)を横に見て、次は2 (N_{low}列)なので、達成できるシステムのPLはb (PL列)であることがわかります。3つのサブシステムがすべてPLbの場合、適合するPLはPLaになります。

PLbシステムと直列サブシステムの組み合わせ

妥当性確認

妥当性確認は、安全システムの開発および試運転の工程を通して重要な役割を果たしています。ISO/EN 13849-2:2003では、妥当性確認に関する要件を設定しています。妥当性確認では、妥当性確認計画を指示しており、テストや故障の木解析、故障モード、効果および致命度解析などの分析技術による妥当性確認について検討しています。これらの要件の多くは、サブシステムのユーザではなく、製造メーカに適用されます。

マシンの立上げ

システムまたはマシン立上げ段階では、安全機能の妥当性確認をすべての動作モードで実行し、すべての正常な状態と予想される異常な状態を網羅する必要があります。入力の組み合わせや操作の順序も考慮しなければなりません。これは、システムが実際の動作および環境特性に適していることを確認するために必ず必要になる重要な手順です。これらの特性の中には、設計段階の予想と異なるものもあります。

IEC/EN 62061に従うシステム設計

IEC/EN 62061 「機械類の安全性- 安全関連電気/電子/プログラム可能電子制御システムの機能安全」は、IEC/EN61508の機械専用の実施です。あらゆるタイプの機械安全関連電気制御システムのシステムレベル設計、およびそれほど複雑でないサブシステムまたは装置の設計にも適用されます。

リスクアセスメントはリスク低減ストラテジになり、さらには安全関連の制御機能の必要性を確認できます。これらの機能を文書化し、以下の内容を含める必要があります。

- 機能要件の仕様
- 安全整合性の要件の仕様

機能要件には、動作頻度、必須応答時間、動作モード、デューティサイクル、動作環境、およびフォルト反応機能などの詳細が含まれます。安全整合性要件は、安全度水準(SIL)というレベルで表されます。システムの複雑さに従って、システム設計が必要なSILを満たしているかを判断するには以下の表の要素の位置またはすべてを考慮する必要があります。

SILの検討項目	シンボル
時間単位当たりの危険側故障が発生する平均確率	PFH_D
ハードウェア・フォルト・トレランス	シンボルなし
安全側故障割	SFF
プルーフテスト間隔	T_1
診断テスト間隔	T_2
共通原因故障(CCF)に対する影響	ß
自己診断率	DC

SILの検討項目

サブシステム

IEC/EN 62061では、「サブシステム」という言葉に特別な意味を持っています。サブシステムはシステムを細分化した場合の最上位の単位であり、サブシステムで発生した故障は安全機能の故障の原因になります。したがって、1つのシステム内で2つの冗長スイッチを使用している場合には、どちらのスイッチも単独ではサブシステムになりません。2つのスイッチと、関連する障害診断機能で1つのサブシステムを構成します。

単位時間当たりの危険側故障が発生する平均確率(PFHD)

IEC/EN 62061は、EN ISO 13849-1のセクションに説明するように同じ基本的な方法を使用して、コンポーネントレベルの故障発生確率を判断できます。同じ対策と方法が、「機構的な」および電子部品に適用します。IEC/EN 62061では、数年のMTTFdを考慮していません。時間当たりの故障発生確率(λ)は、直接計算するか、または以下の式を使用してB10値から取得できます。

λ = 0.1 x C/B10 (この場合、C = 1時間当たりの動作サイクルの回数)

サブシステムまたはシステムの合計PFH_Dを判断する方法については、規格ごとに大きな違いがあります。サブシステムの故障の発生確率を判断するために、コンポーネントの分析を行なう必要があります。共通するサブシステムのアーキテクチャ(後で説明)の計算のために、簡略化した式を提供します。これらの式が適用されない場合には、マルコフモデリングなどのさらに複雑な計算方法を使用する必要があります。各サブシステムの危険側故障発生確率(PFH_D)を互いに加算してから、システムの合計のPFH_Dを決定します。以下の表(規格の表3)を使用して、安全度水準(SIL)がそのPFH_Dの範囲に対応しているかを判断できます。

$$\lambda_{DssB} = (1-\beta)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + \beta \times (\lambda_{De1} + \lambda_{De2}) / 2$$

このアーキテクチャの式では、サブシステム要素の並列配列を考慮するため、前の表から以下の2つの要素を追加します。

β (ベータ)は、共通原因故障(CCF)に対する影響です。

SIL (安全度水準)	PFH_D (単位時間当たりの危険側故障発生確率)
3	10^{-8}以上10^{-7}未満
2	10^{-7}以上10^{-6}未満
1	10^{-6}以上10^{-5}未満

SILの危険側故障発生確率

サブシステムのPFH_Dデータは、通常は製造メーカから提供されます。ロックウェル・オートメーションの安全コンポーネントシステムのデータは、以下を含むいくつかの形式で使用できます：www.discoverrockwellautomation.com/safety

IEC/EN 62061でも、適切な場合、適切な箇所には、信頼性データハンドブックを使用できることを明言しています。

あまり複雑ではない電気機械式のデバイスでは、故障のメカニズムは時間だけよりも、作動の回数と頻度に関連するのが普通です。そのため、これらのコンポーネントについては、このデータは何らかの寿命テスト(EN ISO 13849-1の章に説明するようにB10テストなど)から得られます。B10または同様のデータをPFH_Dに変換するためには、1年当たりの作動回数などのアプリケーションベースの情報が必要です。

注：一般的に、以下のように想定できます(年を時間に変換するには係数を考慮する)。

$PFH_D = 1/MTTFd$

ただし、デュアル・チャネル・システム(診断付き、またはなし)では、1/ PFH_Dを使用してEN ISO 13849-1に要求されるMTTFdを判断することは正しくないことを理解する必要があります。この規格は、1つのチャネルのMTTFd用です。これは、2チャネルのサブシステムの両方のチャネルの組合せのMTTFdとは非常に異なる値です。

アーキテクチャによる制約

IEC/EN 62061の重要な特性は、安全システムをサブシステムに分割することです。サブシステムに付与できるハードウェア安全度水準はPFH_Dだけでは制限できませんが、ハードウェア・フォルト・トレランスとサブシステムの安全側故障割合(SFF)によって制限されます。ハードウェア・フォルト・トレランスは、単一のフォルトが存在しているときにシステムが機能を実行できる能力です。フォルトトレランスが0というのは、単一フォルトが発生した場合、機能が実行されないことを意味します。フォルトトレランスが1のとき、サブシステムは単一フォルトが発生していても機能を実行できます。安全側故障割合(SFF)は、全体的な故障率の中で、危険な故障につながらない故障の割合です。この2つの要素を組み合わせたものが、いわゆるアーキテクチャによる制約で、SIL達成限度(SIL CL)と表されます。以下の表に、アーキテクチャによる制約とSILCLの関係を示します。サブシステム(および、そのシステム)は、規格の他の関連する条項と共に、PFH_D要件とアーキテクチャによる制限の両方を満たす必要があります。

安全側故障割合 (SFF)	ハードウェア・フォルト・トレランス		
	0	1	2
60%未満	特定の例外事項を適用しない限り適用しない	SIL1	SIL2
60～90%	SIL1	SIL2	SIL3
90～99%	SIL2	SIL3	SIL3
99%以上	SIL3	SIL3	SIL3

SILでのアーキテクチャによる制約

例えば、シングル・フォルト・トレランスを備えたサブシステムアーキテクチャと75%の安全側故障割合では、危険側故障割合に関係なく、SIL2定格以下に制限されます。サブシステムを組み合わせているときは、SRCSに適合するSILは、安全関連制御機能に関与するサブシステムの最低のSIL CL以下を備えていなければなりません。

システムの実現

危険側故障の発生確率を計算するには、各安全機能をファンクションブロックに分割する必要があります。これがサブシステムになります。多くの安全機能のシステム設計では、検知装置をロジックデバイスに接続し、そのロジックデバイスをアクチュエータに接続しています。これでサブシステムが直列に配置されます。サブシステムごとに危険側故障割合を決定でき、SIL CLがわかっている場合、システムの故障確率は、サブシステムの故障確率を加算するだけで簡単に計算できます。以下の図に、この概念を示します。

$= PFH_D\,1$ $+ PFH_D\,2$ $+ PFH_D\,3$
$= 1x10^{-7}$ $+ 1x10^{-7}$ $+ 1x10^{-7}$
$= 3x10^{-7}$ 例えば、SIL2に適合する

例えば、SIL 2に適合したいときに、各サブシステムには最低でもSIL 2のSIL CLを付与する必要があり、システムのPFH_Dの合計は前の表に示す許容可能な制限を超えてはなりません。

サブシステム設計 - IEC/EN 62061

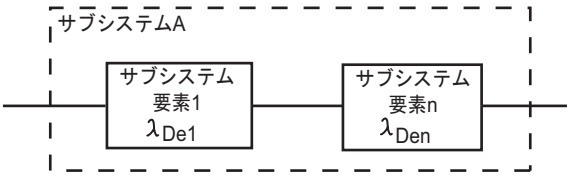
システム設計者は、IEC/EN 62061に従ってサブシステムに「パッケージ化」されているコンポーネントを使用すると、作業がかなり容易になります。これは、サブシステムの設計に特有の要件は適用されないからです。これらの要件は、通常、装置(サブシステム)製造者によって対応され、システムレベルの設計に要求されるものよりはるかに複雑になっています。

IEC/EN 62061では、セーフティPLCなどの複雑なサブシステムがIEC 61508または他の対法する規格に適合することを要求しています。これは、複雑な電子またはプログラマブルコンポーネントを使用する装置の場合、IEC 61508の厳格さがすべて適用されることを意味します。これは非常に困難で、複雑な工程になる可能性があります。例えば、複雑なサブシステムによって実現されたPFHDの評価は、マルコフモデリング、信頼性ブロックダイアグラム、または故障のツリー解析などの手法を使用する非常に複雑なプロセスになる可能性があります。

IEC/EN 62061はそれほど複雑でないサブシステムに関する要件を定めています。通常、これにはインターロックスイッチや電気機械式のモニタ・セーフティ・リレーなどの比較的単純な電気コンポーネントが含まれます。要件は、IEC 6150のような関係性がなく、大変複雑です。

IEC/EN 62061は、4つのサブシステム論理アーキテクチャを提供しています。これと一緒にあまり複雑でないサブシステムによって実現されたPFH$_D$を評価するために使用される付属の式も提供されます。これらのアーキテクチャは純粋に論理的な説明で、物理構造として考えることはできません。4つのサブシステム論理アーキテクチャとそれに付属する式を、以下の4つの図に示します。

以下に示す基本的なサブシステムアーキテクチャの場合、危険側故障の発生確率は互いに追加するだけです。



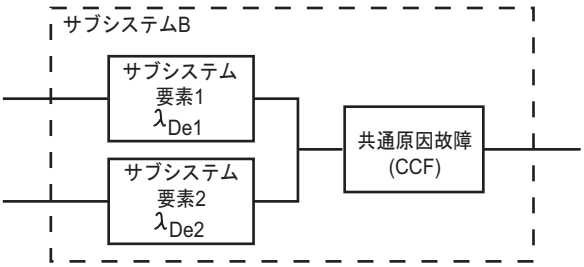
サブシステムの論理的なアーキテクチャA

$$\lambda_{DssA} = \lambda_{De1} + \ldots + \lambda_{Den}$$

$$PFH_{DssA} = \lambda_{DssA} \times 1h$$

λ(ラムダ)は、故障の発生確率を指定するために使用されます。故障の発生確率の単位は、単位時間当たりの故障回数です。λ_Dは、危険側故障発生確率です。λ_{DssA}は、サブシステムAの危険側故障発生確率です。これは、個別の要素e1、e2、e3から最大enまでの故障の発生確率の合計です。危険側故障発生確率に1時間をかけると、1時間当たりの故障発生確率になります。

以下の図に、診断機能なしのシングル・フォルト・トレランスのシステムを示します。アーキテクチャにシングル・フォルト・トレランスが組み込まれている場合、共通原因故障の可能性があるので考慮する必要があります。共通原因故障の派生については、このセクションの後半で詳しく説明します。



サブシステムの論理的なアーキテクチャB

$\lambda_{DssB} = (1-\beta)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + \beta \times (\lambda_{De1} + \lambda_{De2}) / 2$

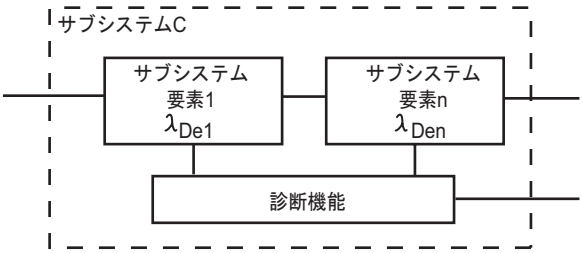
$PFH_{DssB} = \lambda_{DssB} \times 1h$

このアーキテクチャの式では、サブシステム要素の並列配列を考慮するため、前の表から以下の2つの要素を追加します。

β (ベータ) : 共通故障原因(CCF)に対する影響

T1 : プルーフテスト間隔または寿命のいずれか小さいほうです。プルーフテストはフォルトと安全サブシステムの劣化を検出するように設計されています。これによって、サブシステムを動作可能な状態に回復させることができます。実際には、通常、これは交換時期を意味します(EN ISO 13849-1での「活動時間」の用語と同等)。

以下の図に、診断機能を備えた0のフォルト・トレランス・システムの機能を説明します。自己診断率(DC)は、危険側ハードウェア故障発生確率を減らすために使用されます。診断テストは自動的に行なわれます。自己診断率の定義はEN ISO 13849-1と同じで、すべての危険側故障割合に対する検出された危険側故障割合の割合です。



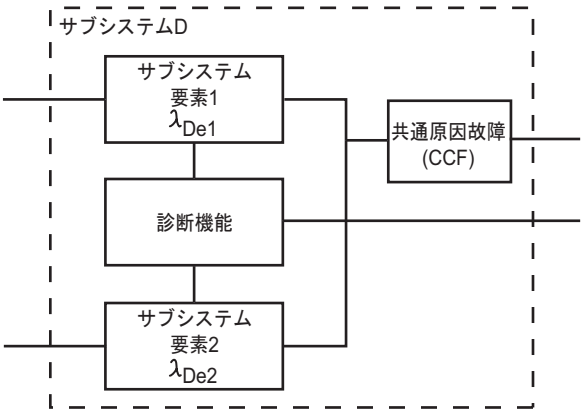
サブシステムの論理的なアーキテクチャC

$$\lambda_{DssC} = \lambda_{De1}(1\text{-}DC_1) + \ldots + \lambda_{Den}(1\text{-}DC_n)$$

$$PFH_{DssC} = \lambda_{DssC} \times 1h$$

これらの式には、サブシステムの要素ごとの自己診断率(DC)が組み込まれています。サブシステムごとの故障の発生確率は、各サブシステムの自己診断率によって低減されます。

以下に、サブシステムのアーキテクチャの4番目の例を示します。このサブシステムはシングル・フォルト・トレランスで、診断機能を備えています。シングル・フォルト・トレランス・システムでは、共通原因故障の発生確率も考慮する必要があります。



サブシステムの論理的なアーキテクチャD

サブシステムの要素が異なる場合は、以下の式を使用します。

$\lambda_{DssD} = (1 - \beta)^2 \{ \lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2) \times T_2 / 2 + \lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 - DC_2) \times T_1 / 2 \} + \beta \times (\lambda_{De1} + \lambda_{De2}) / 2$

$PFH_{DssD} = \lambda_{DssD} \times 1h$

サブシステムの要素が同じ場合は、以下の式を使用します。

$\lambda_{DssD} = (1 - \beta)^2 \{[\lambda_{De}^2 \times 2 \times DC] \times T_2 / 2 + [\lambda_{De}^2 \times \lambda_{De}^2 \times (1-DC)] \times T_1 \} + \beta \times \lambda_{De}$

$PFH_{DssD} = \lambda_{DssD} \times 1h$

両方の式では、1つの追加パラメータT2 (診断テストの間隔)を使用することに注意してください。これは機能の定期的なチェックだけを行なう、プルーフテストより範囲が広くないテストです。

サブシステムの要素が異なる場合の例として、以下の値を想定しています。

$\beta = 0.05$

$\lambda_{De} = 1 \times 10^{-6}$故障/時間

T1 = 87600時間(10年)

T2 = 2時間

DC = 90%

PFH_{DssD} = 5.791E-08 単位時間当たりの危険側故障発生確率
これは、SIL 3に要求される範囲内にあります。

プルーフテスト間隔の影響

IEC/EN 62061は、プルーフテスト間隔(PTI)を20年にすること推奨しています(必須ではない)。プルーフテスト間隔がシステムに与える影響について考えてみます。20年のときにT1で式を再計算すると、結果はPFHDssD = 6.581E-08になります。これは、まだSIL 3に要求される範囲内です。設計者は全体の危険側故障レートを計算するには、このサブシステムと他のサブシステムを組み合わせる必要があることを常に注意してください。

共通原因故障の影響の分析

共通原因故障(CCF)がシステムに与える影響について考えて見ます。追加策を講じて、β (ベータ)値を1% (0,01)に改善して、プルーフテスト間隔を20年のままにします。危険側故障の発生確率が2.71E-08に向上し、これでサブシステムがSIL 3システムに適合できるようになりました。

共通原因故障(CCF)

共通原因故障(CCF)は、1つの原因から複数のフォルトが発生し、危険な故障につながることを意味します。CCFに関する情報が必要になるのは、サブシステム設計者(通常は製造メーカ)だけです。これは、サブシステムのPFH_Dの評価に使用される式の一部として使用されます。通常、システム設計レベルでは必要ありません。

IEC/EN62061の付録Fに、CCFを推定するための簡単な方法が記載されています。以下の表に、スコアリングプロセスの概要を示します。

No.	CCFの対策	スコア
1	隔離/分離	25
2	ダイバーシティ(多様性)	38
3	設計/アプリケーション/経験	2
4	評価/分析	18
5	能力/トレーニング	4
6	環境	18

共通原因故障(CCF)に対する対策のスコアリング

特定のCCF対策を採用するとポイントが得られます。スコアを追加して、以下の表に示すように共通原因故障(β)の要因を決定します。β係数は、すでに説明したように故障の発生確率を調整するためにサブシステムの簡略化されたアーキテクチャの式に使用されます。

全体のスコア	共通原因故障の係数(ß)
<35	10% (0,1)
35 - 65	5% (0,05)
65 - 85	2% (0,02)
85 - 100	1% (0.01)

共通原因故障のベータ係数

自己診断率(DC)

危険側ハードウェア故障割合を減少するために、自動診断テストが採用されています。危険側ハードウェア故障をすべて検出できることが理想ですが、実際的には最大値は99%に設定されます(これは0.99と示すこともできる)。

自己診断率(DC)とは、すべての危険側故障発生確率に対する検出された危険側故障発生確率の割合です。

$$DC = \frac{\text{検出された危険側故障の発生確率}(\lambda_{DD})}{\text{合計の危険側故障発生確率}(\lambda_{Dtotal})}$$

自己診断率は、0～1の値です。

ハードウェア・フォルト・トレランス

ハードウェア・フォルト・トレランスは、危険側故障を発生させずに、サブシステムが耐えることのできるフォルトの数を表します。例えば、ハードウェア・フォルト・トレランスが1であると、2つのフォルトがあると安全関連制御機能の損失につながりますが、1つのフォルトでは損失につながりません。

機能安全の管理

規格には、安全関連電気制御システムを実現するために必要な管理の制御、プロジェクト管理、および技術活動に関して要件が定められています。

プルーフテスト間隔

プルーフテストの間隔は、サブシステムを「新品」の状態にしておくために全面的なチェックまたは交換が必要になる間隔を表します。実際には、機械類に関しては、交換時期を意味します。そのため、プルーフテスト間隔は通常、寿命と同じになります。EN ISO 13849-1:2008では、これは活動時間ともいいます。

プルーフテストは、SRCSのフォルトおよび劣化を検出するチェックで、これによってSRCSをできる限り新品に近い状態に回復させることができます。プルーフテストでは、すべての危険側故障を100%検出する必要があります。チャネルは、個々にテストします。

自動的に行なわれる診断テストと異なり、プルーフテストは通常、手作業によりオフラインで実行されます。自動で行なわれる診断テストは頻繁に実行されますが、それに比べるとプルーフテストはあまり頻繁には行なわれません。例えば、ガードのインターロックスイッチにつながる回路は、診断(パルス)テストで短絡および開回路状態を自動的にテストすることができます。

プルーフテストの間隔は、製造メーカが明確にしなければなりません。場合によっては、製造メーカがさまざまなプルーフテスト間隔を示すことがあります。

安全側故障割合(SFF)

安全側故障割合(SFF)は、自己診断率(DC)と似ていますが、本来安全な状態に終わる傾向のある故障も考慮に入れています。例えば、ヒューズが飛んだ場合、故障は存在しますが、その故障は開回路で、ほとんどの場合は安全な故障であるのは確実です。SFFは、(安全側故障の発生確率と検出できる危険側故障の発生確率の合計)を(安全側故障の発生確率と検出・未検出を合わせた危険側故障の発生確率の合計)で割って計算します。安全機能に何らかの影響を与えるタイプの障害だけを考慮していることに注意してください。

E-stopボタンやインターロックスイッチなどの、ほとんどのあまり複雑ではない機械的なデバイスのSFFは、(単独では)60%未満です。しかし、安全保護のために使用されるほとんどの電気機器は、冗長機能とモニタ機能が組み込まれた設計になっています。したがって、SFFは90%を超えているのが一般的です。

安全側故障割合(SFF)は、以下の式を使用して計算できます。

$$SFF = (\Sigma \lambda_S + \Sigma \lambda_{DD}) / (\Sigma \lambda_S + \Sigma \lambda_D)$$

この場合、

λ_S = 安全側故障の発生確率

$\Sigma\lambda_S + \Sigma \lambda_D$ = 全体の故障の発生確率

λ_{DD} = 検出された危険側故障の発生確率

λ_D = 危険側故障の発生確率

系統的故障

規格には、系統的故障の制御および回避に関する要件が記述されています。系統的故障はランダムハードウェア故障とは異なります。ランダムハードウェア故障は、通常、ハードウェアの部品の劣化が原因で時間的に無秩序に発生する故障です。
典型的な系統的故障のタイプは、ソフトウェア設計エラー、ハードウェア設計エラー、要件仕様エラー、および任意の手順などです。系統的故障を回避するために必要な手順の例を以下に示します。

- コンポーネントを適切に選択、組合せ、配置、組立て、および取付ける。
- 優れた技術的手法を使用する。
- 製造メーカの仕様および取付け手順に従う。
- コンポーネント間の互換性を確認する。
- 環境条件への耐性を考慮する。
- 適切な材質を使用する。

安全関連制御システムの構造に関する注意事項

概要

このセクションでは、規格に対して安全関連制御システムを設計する際に考慮する必要がある、一般的な構造に関する注意事項と原理について考えます。カテゴリは主に制御システムの構造を扱うため、古いEN 954-1ではカテゴリという用語をよく使用しています。

制御システムのカテゴリ

制御システムの「カテゴリ」は、前のEN 954-1:1996 (ISO13849-1:1999)に基づいています。ただし、この用語は安全制御システムを説明するためにまだ頻繁に使用されており、「制御システムの機能安全の概要」セクションに記載されているようにEN ISO13849-1の不可欠な部分です。

安全関連制御システムのフォルトの応答性能を説明する、5つのカテゴリがあります。これらのカテゴリのまとめについては、次ページの表を参照してください。以下の注記はその表に適用されます。

注1：カテゴリB自体には安全に関する特別な手段はなく、他のカテゴリの基盤になります。

注2：共通の原因によって、または最初のフォルトの結果として発生した複数のフォルトは、1つのフォルトとしてカウントします。

注3：フォルトの検査は関連する2つのフォルト(証明できる場合)に制限されますが、複雑な回路(マイクロプロセッサ回路など)では、より多くの関連するフォルトの検討が必要になることがあります。

カテゴリ1は、フォルトの防止が目的です。これは、適切な設計原理、構成部品、および材質を使用することで達成されます。原理と設計の簡潔さに加え、安定した予測可能な材料特性がこのカテゴリの鍵となります。

カテゴリ2、3、および4では、フォルトを防止できない場合、それを検出して適切に対応することが要求されます。

これらのカテゴリでは、冗長、多様化、モニタ機能が重要になります。冗長は同じ手法の二重化です。多様化は2種類の異なる方法を使用します。モニタ機能は、デバイスの状態をチェックし、状態に応じて適切な処置を行ないます。安全重視機能を二重化し、その動作を比較する方法が一般的なモニタ方法ですが、その他の方法もあります。

要件のまとめ	システムの動作
カテゴリB (注1を参照) そのコンポーネントと同様に、マシン制御システムの安全関連部分またはそれらの保護機器の予想される影響に抵抗できるように、安全関連部分を、関連する規格に従って設計、建造、選択、組立て、および組み合わせる必要がある。基本的な安全原理を適用する必要がある。	フォルトが発生したときに、安全機能の損失につながることがある。
カテゴリ1 カテゴリBの要件を、実績のある安全コンポーネントと安全原理の使用と共に適用する。	カテゴリBについて説明する通りですが、安全関連機能の安全関連の信頼性がより高くなる(信頼性を高めると、フォルトの可能性小さくなる)。
カテゴリ2 カテゴリBの要件と実績のある安全原理の使用を適用する。安全機能は、マシン制御システムによってマシンの始動時と周期的にチェックされる。フォルトが検出されると安全状態が起動されるか、またはこれが使用できないときは警告が行なわれる必要がある。EN ISO 13849-1は、テスト頻度が少なくとも需要頻度である100回より多い頻度であることを前提としている。EN ISO 13849-1は、外部テスト機器のMTTFdが、テストしている動作機器のMTTFdの半分よりも大きいことを前提としている。	チェックによって安全機能の損失が検出される。フォルトの発生は、チェック期間の安全機能の損失につながることがある。
カテゴリ3 (注2 & 3を参照) カテゴリBの要件と実績のある安全原理の使用を適用する。その部分のいずれか1つのフォルトが安全機能の損失につながらないように、システムを設計する必要がある。実施可能であれば、1つのフォルトが検出される。	1つのフォルトが発生したときに、安全機能が必ず実行される。一部のフォルト(すべてではない)が検出される。検出されないフォルトの蓄積によって、安全機能の損失につながることがある。
カテゴリ4 (注2 & 3を参照) カテゴリBの要件の要件と実績のある安全原理の使用を適用する。その部分のいずれか1つのフォルトが安全機能の損失につながらないように、システムを設計する必要がある。安全機能の次の要求時またはその前に、1つのフォルトが検出される。この検出をできないときは、フォルトの蓄積は安全機能の損失につながらない。	フォルトが発生したときに、安全機能は必ず実行される。将来的な安全機能の損失を防ぐためにフォルトが検出される。

カテゴリB

カテゴリBは、安全関連制御システムも、安全関連ではない制御システムも含め、あらゆる制御システムの基本要件を示します。制御システムは予定された環境で機能する必要あります。信頼性は、装置が予定された状況下で指定された間隔で意図した機能を実行できる可能性として定義されているので、信頼性の概念は制御システムの基盤になります。

カテゴリBでは、基本的な安全原則の適用を求めています。ISO 13849-2は、電気、空圧、油圧、および機械システムの基本的な安全原理を明記しています。電気原理の概要は以下の通りです。

- 適切な選択、組合せ、配置、組立て、および設置(制御メーカの手順書に従う。)
- 構成部品の電圧および電流の整合性
- 環境条件に対する耐性
- 電源遮断の原則の使用
- 過渡抑制
- 応答時間の短縮
- 予期しない始動に対する保護
- 入力装置の確実な取付け(例えば、インターロックの取付け)
- 制御回路の保護(NFPA79 & IEC60204-1に従う。)
- 適切な保護用のボンディング

設計者は製造メーカから提供される取付け手順書に従ってデバイスの選択、設置、組立てを行なわなければなりません。これらのデバイスは、指定された電圧および電流定格内で動作する必要があります。電磁適合性、振動、衝撃、汚染、洗浄などの環境条件に対する指定も考慮する必要があります。電源遮断の原則が使用されます。コンタクタコイル間に過渡保護が取付けられます。モータは過負荷から保護されます。配線および接地はすべて適切な電気規格に適合しています。

カテゴリ1

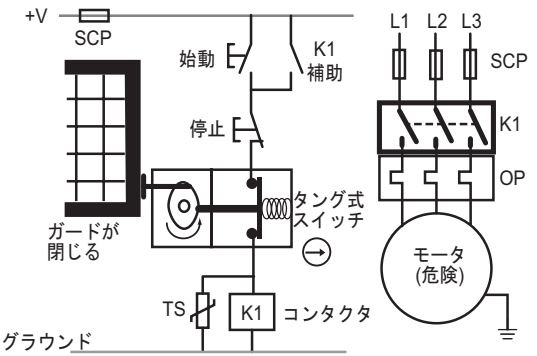
カテゴリ1は、カテゴリBの条件を満たし、実績のある安全構成部品を使用するように求めています。具体的にどれが安全構成部品で、実績があるかどうかはどのように判断するのでしょう? ISO 13849-2では、機械、空圧、油圧、および電気システムに関してこれらの疑問に答えています。付録Dは電気構成部品について取り上げています。

多数の類似したアプリケーションで問題なく使用されていれば、そのコンポーネントは実績があると見なされます。新たに設計された安全コンポーネントは、適切な規格に準拠して設計されれ、検証されていれば、実績があると考えられます。以下の表に、いくつかの電気部品とそれに関連する規格を示します。

実績のあるコンポーネント	規格
ポジティブモード作動(直接開動作)のスイッチ	IEC 60947-5-1
非常停止装置	ISO 13850, IEC60947-5-5
ヒューズ	IEC 60269-1
サーキットブレーカ	IEC 60947-2
コンタクタ	IEC 60947-4-1, IEC 60947-5-1
機械的にリンクされた接点	IEC 60947-5-1
補助コンタクタ(例えば、コンタクタ、制御リレー、強制開離リレー)	EN 50205, IEC 60204‑1, IEC 60947‑5‑1
トランス	IEC 60742
ケーブル	IEC 60204-1
インターロック	ISO 14119
温度スイッチ	IEC 60947-5-1
圧力スイッチ	IEC 60947-5-1 + 空圧または油圧要件
制御および保護用の切換えデバイスまたは装置(CPS)	IEC 60947-6-2
プログラマブル・ロジック・コントローラ	IEC 61508, IEC 62061

安全関連制御システムの構造に関する注意事項

実績のあるコンポーネントをカテゴリBシステムに適用すると、リミットスイッチは直接開動作のタング式スイッチと交換され、コンタクタは溶着接点に対する保護を強化するために大きくなりすぎます。



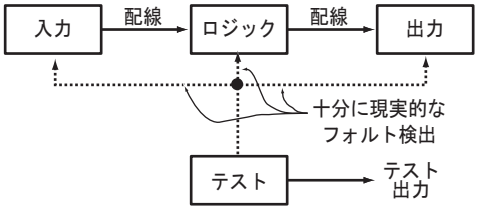
シンプルなカテゴリ1の安全システム

ここに示す図では、単純なカテゴリBのシステムをカテゴリ1に適合するために変更しています。インターロックおよびコンタクタは、危険箇所にアクセスする必要がある場合、アクチュエータからエネルギーを除去するために重要な役割を果たします。タング式インターロックは、直接開動作接点に関するIEC60947-5-1の要件を満たしています。適合していることは、円の中に矢印が描かれたマークで示されます。実績のあるコンポーネントを使用すると、カテゴリBの場合よりカテゴリ1の方がエネルギーが除去される可能性が高くなります。実績のあるコンポーネントを使用する目的は、安全機能が失われないようにすることです。これらの改善を行なっても、1つのフォルトで安全機能の損失につながることがあります。

カテゴリBおよび1の基本は防止です。設計では危険な状況を防ぐことを目的とします。防止策だけではリスクを十分に軽減できない場合は、フォルト検出を使用する必要があります。カテゴリ2、3、および4は、フォルト検出が基本で、より高レベルのリスク削減を実現するために要件はしだいに厳しくなります。

カテゴリ2

カテゴリBの要件を満たすだけではなく、実績のある安全原理を使用して、安全システムはカテゴリ2を満たすための適合テストを受けている必要があります。このテストは、制御システムの安全関連部品内のフォルトを検出できるように構成されています。フォルトが検出されなければ、マシンは動作できるようになります。フォルトが検出された場合は、テストでコマンドを起動する必要があります。可能な場合は、そのコマンドでマシンを安全状態にする必要があります。



テストでは、十分に現実的なフォルト検出を行なわなければなりません。テストを行なう装置は、安全システムと一体化している場合も、独立した装置の場合もあります。

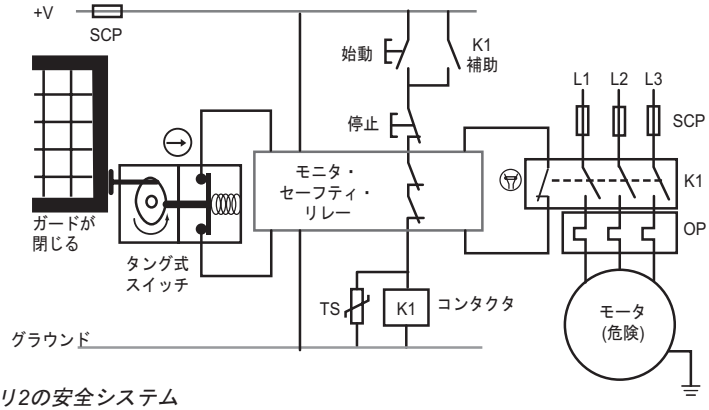
テストは、以下のとき行なう必要があります。

- マシンに最初に電源を投入したとき
- 危険な作業を開始する前
- リスクアセスメントで必要と見なされた場合は、定期的に

注：EN ISO 138491-1は、100:1の安全機能の需要割当に対するテストを想定しています。ここに示す例はそのような機器には適合しません。

「可能な限り」および「十分に現実的」という言葉は、すべてのフォルトを検出できるとは限らないことを意味しています。これはシングル・チャネル・システム(入力、ロジック、出力の各装置を1本のワイヤで接続)であるため、1つのフォルトでも安全機能の損失につながることがあります。場合によっては、すべてのコンポーネントをチェックできないために、カテゴリ2を安全システムに完全に適用できないこともあります。

安全関連制御システムの構造に関する注意事項

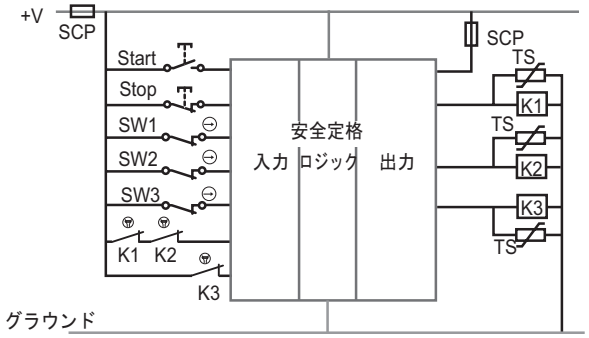


カテゴリ2の安全システム

上図では、シンプルなカテゴリ1システムをカテゴリ2に適合するように拡張しています。モニタ・セーフティ・リレー(MSR)にはテストを実行する機能があります。電源投入時に、MSRは内部コンポーネントをチェックします。フォルトが何も検出されないときは、MSRはその接点のサイクルをモニタすることでタング式スイッチをチェックします。フォルトが何も検出されず、ガードが閉じたときは、MSRは、コンタクタの機械的にリンクされた接点について出力デバイスをチェックします。フォルトが何も検出されずコンタクタがオフしたときは、MSRは内部出力をオンして、K1のコイルを停止ボタンに接続します。この次点で、マシン制御システムの安全定格では内部分である始動/停止/インターロック回路は、マシンのオンとオフを切換えられるようになります。

ガードが開くとMSRの出力がオフします。ガードが再度閉じると、MSRは安全システムのチェックを繰返します。フォルトが何も検出されないときは、MSRはその内部出力をオンします。MSRは、入力デバイス、ロジックデバイス(自身)、および出力デバイスでテストを実行することによって、この回路がカテゴリ2に適合するようにできます。テストは、最初の電源投入時と危険の起動前に実行できます。

本来の論理機能を使用することにより、セーフティPLC (IEC 61508に対するPLC安全定格)ベースの安全システムは、カテゴリ2を満たすように設計することができます。上述のカテゴリ1のように、PLC (そのテスト能力を含む)の十分に試した正当化が課題になります。カテゴリ2定格を必要とする複雑な安全システムの場合は、IEC 61508に対するPLC安全定格を、非安全定格PLCに置き換える必要があります。



複雑なカテゴリ2の安全システム

上図に、安全定格PLCを使用する複雑なシステムの例を示します。安全定格PLCは、適切な規格に合わせて設計されているので、実績に関する要件を満たしています。コンタクタの機械的にリンクされた接点は、テストのためにPLCの入力に接続されます。これらの接点は、プログラムロジックによって1つの入力端子に直列に接続されるか、または個々の入力端子に接続されます。

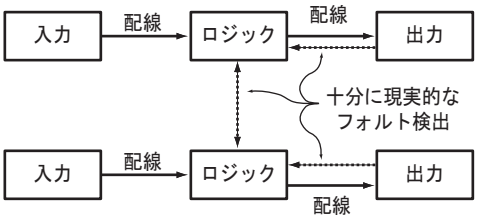
実績のある安全関連部品を使用していても、チェック間で1つのフォルトが起こると安全機能の損失につながる恐れがあります。そのため、カテゴリ2システムは、リスクの低いアプリケーションで使用されます。より高レベルのフォルトトレランスが要求される場合、安全システムはカテゴリ3または4を満たす必要があります。

カテゴリ3

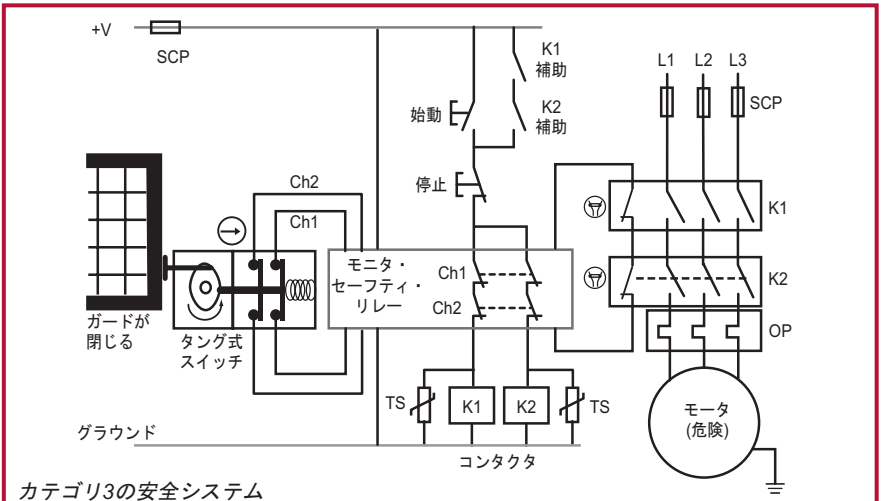
カテゴリBの要件を満たして、実績のある安全原理を使用しているだけではなく、カテゴリ3では、1つのフォルトが存在しても安全機能を正常に実行できることが要求されます。安全機能に次の要求が出されたとき、または要求か出される前に可能な限りフォルトの検出を行なう必要があります。

ここでも「可能な限り」という表現が使われます。これは、検出されない可能性のあるフォルトを対象としています。検出されなかったフォルトが安全機能の損失につながらない限り、安全機能はカテゴリ3に適合できます。その結果、未検出フォルトの蓄積が安全機能の損失につながる可能性があります。

安全関連制御システムの構造に関する注意事項



これは、カテゴリ3システムの原理を説明するブロックダイアグラムです。実行可能なクロスモニタ機能および出力モニタ機能と冗長を組み合わせて使用すると、安全機能を確実に実行できるようになります。



カテゴリ3の安全システム

上図に、カテゴリ3システムの例を示します。接点の冗長セットがタング式インターロックスイッチに追加されています。内部には相互にクロスモニタする冗長回路がモニタ・セーフティ・リレー(MSR)に組み込まれています。コンタクタの冗長セットはモータから電力を除去します。コンタクタは、実行可能な機械的にリンクされた接点を介してMSRによってモニタされます。

フォルト検出、安全システムの各部分だけでなく、接続(つまりシステム)についても考慮する必要があります。デュアル・チャネル・タング式スイッチの故障モードとはどのようなものか?、MSRの故障モードとはどのようなものか?、コンタクタK1およびK2の故障モードとはどのようなものか?、配線の故障モードとはどのようなものか?

タング式インターロックスイッチは、直接開接点を使用して設計されています。したがって、ガードを開くと、溶着した接点が開くように設計されているのがわかります。これによって、1つの故障モードが解決されます。他の障害モードは存在するのでしょうか?直接接開動作スイッチは、通常、スプリングの力で戻るように設計されています。ヘッドが取り外されたり、壊れたりした場合は、安全接点がスプリングの力で閉じた(安全な)状態に戻されます。ほとんどのインターロックスイッチは、取り外し可能なヘッドを使用して、さまざまなアプリケーションの設置要件に対応できるように設計されています。ヘッドは取り外したり、2〜4つの位置で回転させることができます。

ヘッドの取付けねじが正しく締め付けられていないと、障害が発生する可能性があります。この状況では、予想されるマシンの振動によりヘッドの取付けねじが抜ける可能性があります。スプリング圧が掛かっている操作ヘッドは安全接点から圧力を取り除くので、安全接点が閉じます。その後、ガードを開いても安全接点は開かず、危険につながる障害が発生します。

同様に、スイッチ内の動作メカニズムを確認する必要があります。1つのコンポーネントの故障が安全機能の損失につながる確率はどの程度でしょう。一般的な方法は、カテゴリ3の回路でデュアル接点のタング式インターロックを使用する方法です。この方法は、スイッチの単一の故障を排除して安全接点を開く方法をベースにします。これは、「フォルトの排除」と考えられ、これについてはこの後に説明します。

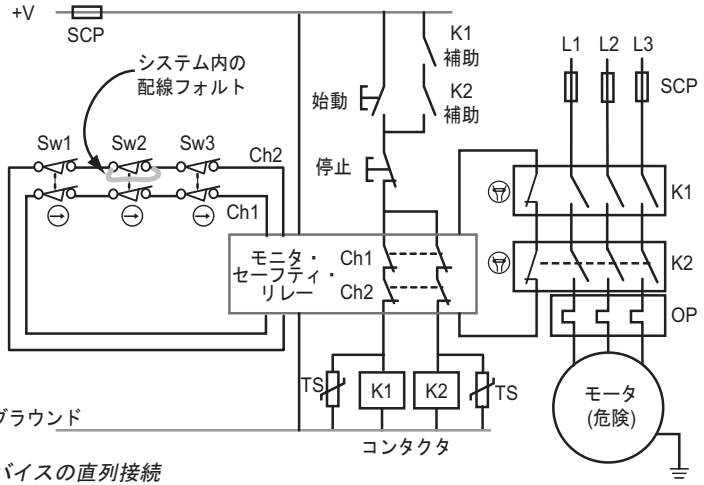
モニタ・セーフティ・リレー(MSR)はサードパーティによって評価され、カテゴリレベル(またはPLおよびSIL CL)を割付けられることの多い、複雑さを抑えた装置です。通常、MSRにはデュアルチャネル機能、クロス・チャネル・モニタ機能、外部装置モニタ機能、短絡保護が組み込まれます。モニタ・セーフティ・リレーの設計や使用方法に関する指示が書かれた特別な規格はありません。MSRは安全機能の実行能力をISO13849-1またはその前のEN 954-1によって評価されます。システムの安全カテゴリ定格を満たすために、MSRは、同じかまたはそれ以上の定格を持っている必要があります。

2つのコンタクタが出力装置による安全機能の実現を確実なものにします。過負荷保護と短絡保護により、溶着接点によってコンタクタが故障する可能性は小さくなりますが、可能性がないわけではありません。コンタクタは、スタックアマチャが原因で電源切換え接点が閉じた場合も故障することがあります。1つのコンタクタが故障して危険な状態になると、もう1つのコンタクタが危険箇所から電力を除去します。MSRは、次のマシンサイクルでフォルトが発生したコンタクタを検出します。ゲートが閉じているときに始動ボタンが押されると、故障したコンタクタの機械的に接続された接点は開いたままになり、MSRは安全接点を閉じることができないため、フォルトが明らかになります。

検出されないフォルト

カテゴリ3システムの構造では、フォルトの中には検出できないものもあります。これらのフォルトだけでは、安全機能の損失にはつながりません。

フォルトを検出できる場合に、特定の状況で、システム構造内の他のデバイスの動作によってマスクされているか、または意図せずにクリアされることがあるかを知っておく必要があります。



入力デバイスの直列接続

上図に、複数の装置をモニタ・セーフティ・リレーに接続するために広く使用されている方法を示します。各装置には、通常閉直接開動作接点が2つ組み込まれています。これらの装置には、インターロックまたは非常停止ボタンを組み合わせて使用できます。この方法では、入力装置はデイジーチェーン接続されるので、配線コストを節約できます。示すようにSw2の接点の1つで短絡フォルトが発生すると仮定します。このフォルトを検出できますか?

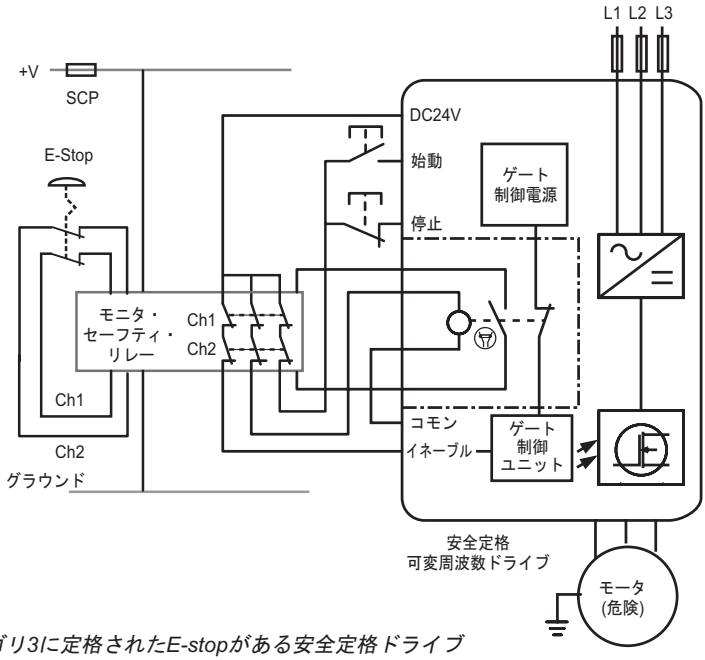
スイッチSw1 (またはSw3)が開くと、Ch1とCh2の両方が回路を開き、MSRが危険箇所から電力を除去します。その後、Sw3が開いてから再度閉じても、MSRのステータスが変わっていないためその接点間のフォルトは検出されず、Ch1とCh2の両方が開いたままになります。Sw1 (またはSw3)が閉じると、始動ボタンを押して危険箇所を再起動できできます。これらの状況では、フォルトによって安全機能が失われることはありませんが、検出されずシステム内に存在するままになり、その後のフォルト(Sw2の2番目の接点での短絡)によって安全機能が失われることになります。

Sw2だけが開くいてから閉じて、他のスイッチが動作しない場合、Ch1は開いてCh2は閉じたままになります。MSRは、Ch1が開いたため危険箇所の電力を除去します。Sw2が閉じると、Ch2が開いていないため始動ボタンを押してもモータは始動できません。フォルトが検出されます。ただし、何らかの理由でSw1 (またはSw3)が開いてから閉じると、Ch1とCh2の両方が開いてから回路を閉じます。このシーケンスは、フォルトのクリアに似ていて、MSRで意図しないリセットが起こることがあります。

EN ISO 13849-1またはIEC 62061を使用しているときに、DCがこの構造内の個々のスイッチに何を求めるかという質問があがります。本書の発行時点では、これには特に決定的なガイダンスはありませんが、スイッチが適合する期間フォルトを公開することが個別にテストされている状態では、DCを60%であると想定することは普通で妥当性があります。スイッチの1つ(または複数)は個別にテストされていないことが予測できるときは、そのDCが0であるべきかを検討できます。本書の発行時点では、EN ISO 13849-2は改定されています。発行時には、この問題についてもっと多くのガイダンスを記載しているかもしれません。

機械的な接点の直列接続は、フォルトの蓄積によって安全機能の損失につながることがあるのでカテゴリ3に制限されています。実際には、DC (および、そのためにSFF)を低減すると、達成可能な最大のPLとSILがPLdとSIL2に制限されます。

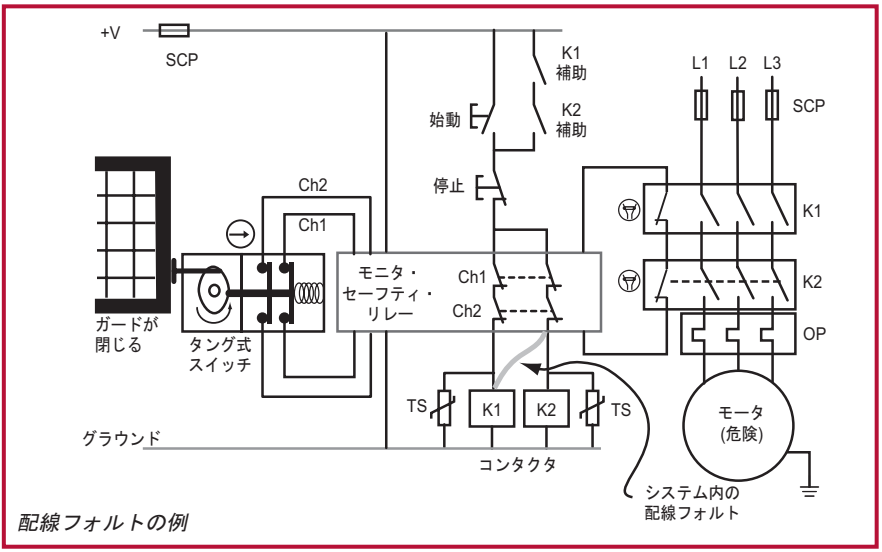
興味深いのは、カテゴリ3構造のこれらの特性を常に考慮する必要があるが、新しい機能安全規格ではかなり絞られていることです。



カテゴリ3に定格されたE-stopがある安全定格ドライブ

上図に、安全定格の可変周波数ドライブを使用するカテゴリ3回路を示します。ドライブ技術の最近の成果EN/IEC 60204-1とNFPA79規格規格の更新が加わって、アクチュエータに電気機械式のディスコネクト(例えば、モータ)がなくても安全定格ドライブを非常停止回路で使用できるようになりました。

E-Stopを押すと、MSRの出力が開きます。これによって、停止信号をドライブに送り、イネーブル信号を除去して、ゲート制御電源が開きます。ドライブは、カテゴリ0停止を実行して、モータへの電力を直ちに遮断します。この機能は「安全トルクオフ」といいます。ドライブは、モータへの電力を除去するために、イネーブル信号と強制開離リレー信号という冗長信号を使用するので、カテゴリ3を実現できます。強制開離リレーは、アクチュエータへの合理的で実際的なフィードバックを提供します。ドライブ自体は、1つのフォルトが安全機能の損失につながらないと判断するために分析されます。

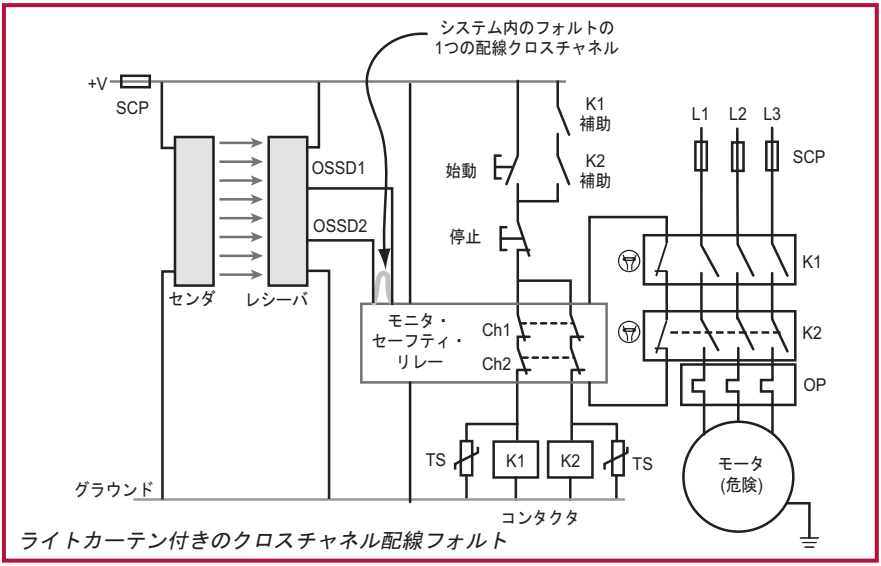


配線フォルトの例

上図に、MSRのチャネル2の安全出力からコンタクタK1コイルへの配線フォルト、短絡の例を示します。すべてのコンポーネントは適切に動作しています。この配線フォルトは機械の稼働前またはその後の拡張またはメンテナンス中に発生する可能性があります。

このフォルトは検出可能ですか?

このフォルトは、図に示すように安全システムによって検出されません。幸い、これは安全機能の損失にはつながりません。このフォルトだけでなく、Ch1とK2間のフォルトは、立上げ中または次の保守作業中に検出する必要があります。EN ISO 13849-2の付録Dの表D4に記載されたフォルト排除の可能性があるリストには、機器が電気的なエンクロージャ内にあり、エンクロージャと配線の両方IEC/EN 60204-1の要件を満たしているときに、これらのタイプのフォルトを排除できるかを明確にします。EN ISO 13849-1およびIEC 62061の合同技術報告書にも、PLeとSIL3までであるとみなされるこのフォルト排除を明確にしています。これは、カテゴリ4でも使用できます。



ライトカーテン付きのクロスチャネル配線フォルト

上図には、ライトカーテンを使用する安全システムの例を示します(OSSD出力)。

*安全システム**はこのフォルトを検出できますか**?*

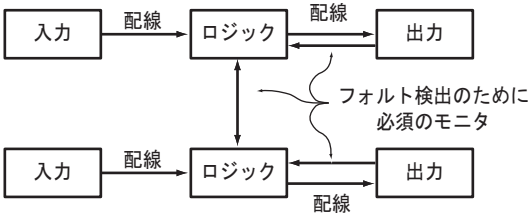
MSRは、両方の入力が+Vにプルアップされるためこのフォルトを検出できません。この例では、配線フォルトはライトカーテンによって検出されます。一部のライトカーテンは、パルステストと呼ばれるフォルト検出技術を使用してます。これらのライトカーテンによって、フォルトがすぐに検出され、ライトカーテンはその出力をオフします。つまり、ライトカーテンがクリアされていると検出が行なわれます。ライトカーテンがその出力をオンにしようとするときは、フォルトが検出されて、出力はオフのままになります。いずれにせよ、フォルトが存在する危険箇所がオフのままになります。

パルステストによるフォルト検出

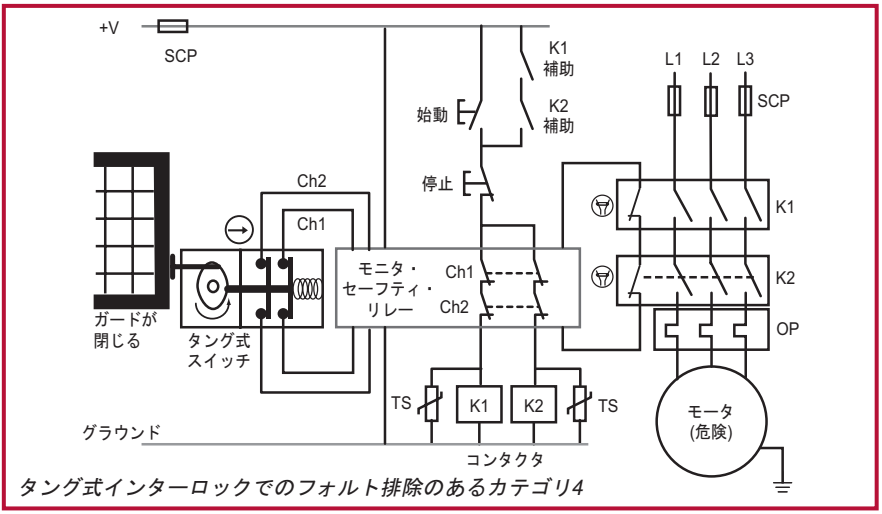
安全回路は、安全システムがアクティブで危険箇所が保護されているときに電流を流すように設計されています。パルステストは、極めて短期間、回路電流を0に降下する手法です。この間隔は、安全回路が応答して危険箇所をオフにするには短すぎ、マイクロプロセッサベースのシステムが検出するために十分な長さです。チャネル上のパルスは、相互にオフセットされています。クロスフォルト短絡が発生した場合に、マイクロプロセッサは両方のチャネルでパルスを検出して、危険箇所をオフにするコマンドを開始します。

カテゴリ4

カテゴリ3と同様に、カテゴリ4では安全システムがカテゴリBの安全原則に適合して、単一フォルトが存在するときに安全機能を実行できることが要求されます。フォルトの蓄積が安全機能の損失につながる可能性のあるカテゴリ3と異なり、カテゴリ4ではフォルトが蓄積された状態でも、安全機能を実行できることが要求されます。フォルトの蓄積について考慮する場合、2つのフォルトでも十分ですが、設計によっては3つのフォルトが必要な場合もあります。



ここに示すのは、カテゴリ4のブロックダイアグラムです。両方の出力デバイスのモニタとクロスモニタは、十分に実用的な場合だけでなく、基本的に必須です。これによって、カテゴリ4とカテゴリ3が区別されます。

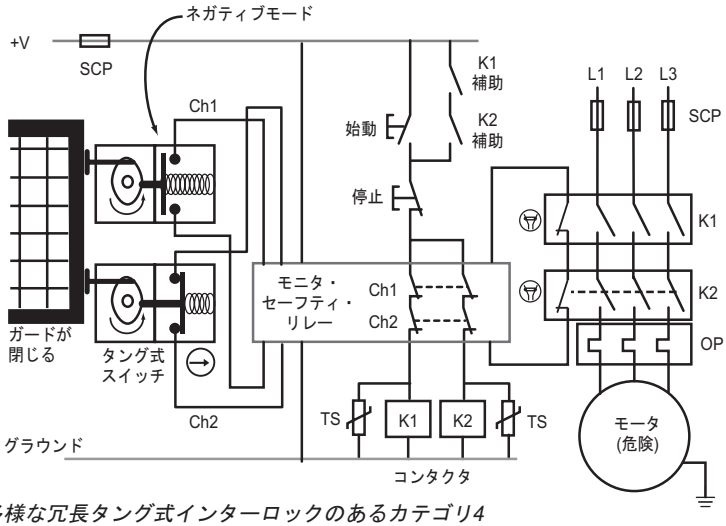


タング式インターロックでのフォルト排除のあるカテゴリ4

上図には、タング式インターロックでフォルト排除を使用するカテゴリ4回路の例を示します。フォルト排除によって、タング式インターロック接点が開かなくなることを考慮する必要がなくなります。フォルト排除は、技術的に証明して文書化する必要があります。アクチュエータ速度、アクチュエータの配置、機械的な定義、および操作ヘッドの保護を、証明する際に考慮する必要があります。

安全システムの設計者がタング式インターロックを使用したいが、インターロックでフォルト排除を簡単に使用できないときは、カテゴリ4を満たすために2つのタング式インターロックを使用できます。モニタ・セーフティ・リレー自体がカテゴリ4を満たすように定格されていることが必要で、機械的にリンクされた接点を使用する両方の出力コンタクタをモニタする必要があります。

コモンモードまたは共通原因故障による安全機能の損失の可能性をさらに減らすために多様性を適用でき、タング式インターロックスイッチの1つをネガティブモードに変換できます。ネガティブモードで作動する1つのスイッチを使用でき、2番目のスイッチは直接開作動接点を使用します。以下の図に、この多種多様な方法の例を示します。この方式では、通常開と通常閉入力を使用できるようにMSRを設計していなければなりません。



多種多様な冗長タング式インターロックのあるカテゴリ4

コンポーネントおよびシステム定格

カテゴリは、システム定格と同様に安全関連部品(デバイス)定格の一部として使用できます。これによって生じる多少の混乱は、コンポーネントとその機能を理解することで解明できます。前述の例を学習することによって、カテゴリ1に定格されたインターロックスイッチなどのコンポーネントをカテゴリ1システム内に使用でき、追加のモニタ機能を提供するときにカテゴリ2システムに使用できることがわかります。2つのコンポーネントがモニタ・セーフティ・リレーで提供される診断機能と互いに使用されているときは、カテゴリ3または4システムの一部を形成することもできます。

モニタ・セーフティ・リレーおよびプログラマブル・セーフティ・コントローラなどの一部のコンポーネントには独自の内部診断があり、適切な性能を保証するためにチェックできます。そのため、追加手段なしでカテゴリ2、3、または4に適合するように安全コンポーネントとして定格できます。

フォルトに関する注意事項

安全分析には、詳しいフォルトの分析と、フォルトが存在するときの安全システムの動作について完全に理解していることが必要です。ISO 13849-1とISO 13849-2では、フォルトの検討とフォルトの排除について詳細に説明しています。

フォルトがその後のコンポーネントの障害を招く場合、最初のフォルトとそれに続くすべてのフォルトは単一のフォルトと考えられます。

1つの原因の結果として複数のフォルトが発生する場合、そのフォルトは単一のフォルトと考えられます。これは、共通原因故障と呼ばれます。

2つ以上のフォルトが同時に発生することは、ほとんどあり得ないので、この分析では考慮されません。機能を使用する期間が過度に長くない場合に、安全機能に出される要求の間では、1つのフォルトだけが発生するということが基本的な条件です。

フォルト排除

オリジナルのEN 954-1と、最近のEN ISO 13849-1とIEC 62061はすべて、障害が発生する見込みがほとんどないことを示している場合、安全システム分類を決定する際にフォルト排除の使用を認めています。フォルト排除が使用されている場所で、その排除が適切に妥当であることと安全システムの計画されたライフタイムに対して排除が有効であることを把握しておくことは重要です。安全システムによって保護されるリスクのレベルが高くなると、フォルト排除で必要となる妥当性がより厳格になります。これは、特定のタイプのフォルト排除がいつ使用できるかできないかについて、何らかの混乱を生ずる原因となります。ここで説明するように、最新の規格とガイダンスの文書でこの問題についていくつかの見方を明記しています。

一般的に、安全システムにより実装される安全機能にPLeまたはSIL3が指定される場合、このレベルのパフォーマンスを達成するためにフォルト排除のみに頼ることは普通ではありません。これは、使用されるテクノロジおよび対象となる動作環境によって左右されます。したがって、設計者がPLまたはSILを増すためにフォルト排除の使用についてさらに注意を払う必要があります。例えば、フォルト排除の使用は、PLeやSIL3システムを実現するために、電気機械式位置スイッチや手動作動スイッチ(非常停止装置など)の機械的観点には適用されません。特定の機械的なフォルト状態(磨耗/腐食、破断など)に適用可能なこれらのフォルト排除は、ISO 13849-2の表A.4で説明されています。したがって、PLeまたはSIL3を実現するために必要なガード・インターロック・システムでは、スイッチアクチュエータの破損などのフォルトを排除することが通常は妥当とは認められないため、このレベルのパフォーマンスに達成するために、最小フォルトトレランス1 (例えば、2つの従来型の機械式位置スイッチ)を組込む必要があります。ただし、関連する規格に従って設計された制御パネル内の配線の短絡などのフォルトを排除するために、これは許容することができます。

フォルト排除の使用については、EN ISO 13849-2の改訂版に記載予定です。

IEC/EN 60204-1およびNFPA 79に従う停止カテゴリ

安全関連制御システムに関連する「カテゴリ」という用語には、2つの異なる意味があるために不運と混乱をまねくことがあります。もともとは、EN 954-1でカテゴリについて説明しています。これは、フォルト状態での安全システムの性能を分類したものです。

また、もとのIEC/EN 60204-1およびNFPA 79で、「停止カテゴリ」と明示されてます。停止カテゴリには、以下の3つがあります。

停止カテゴリ0では、アクチュエータへの電力供給をすぐに遮断する必要があります。場合によって、これは非制御型停止と見なされます。というのも、一部の環境では、モータは惰性で回転し続けるため、動作が停止するのにある程度の時間がかかるからです。

停止カテゴリ1では、ブレーキを作動させるため停止するまでアクチュエータへの電力供給を継続させる必要があり、停止後にアクチュエータへの電力供給を遮断します。

停止カテゴリ2では、アクチュエータから電力供給を遮断する必要はありません。

非常停止としては、停止カテゴリ0または1しか使用できないことに注意してください。2つのカテゴリのどちらを使用すべきかは、リスクアセスメントによって決定されます。

ここで示すすべての回路の例は、停止カテゴリ0を使用しています。停止カテゴリ1は、最終的な電力供給の停止による時間遅延出力によって停止します。ガードロックのあるインターロックガードには、カテゴリ1の停止システムがついていることが多くあります。この場合、マシンが安全(つまり停止)状態になるまで、ガードを閉じた位置にロックします。

プログラマブルコントローラについて十分に検討しないままマシンを停止すると、再始動に影響を与えたり、ツールやマシンに深刻な損傷が発生する可能性があります。標準のPLC (セーフティPLC以外)は、安全関連の停止作業には関わらないので、他の方法を考える必要があります。

以下に、考えられる2つのソリューションを示します。

1. 時間遅延オーバライドコマンド付きのセーフティリレー

即時作動式と遅延作動式の両方の出力のあるセーフティリレーが使用されます。即時作動式の出力はプログラム可能な装置(例：PLC)の入力に接続され、遅延作動式の出力はコンタクタに接続されます。ガード･インターロック･スイッチが作動すると、セーフティ・リレー・スイッチの即時出力がオンになります。これで、プログラム可能なシステムは正しいシーケンスで停止を行なうために信号を送ります。このプロセスを行なうために十分な時間が経過してから、セーフティリレーの遅延出力がオンになり、メインコンタクタを遮断します。

注：全体的な停止時間を判断するための計算では、セーフティリレー出力遅延期間も考慮する必要があります。このことは、安全距離の計算に従って装置の位置を決定するためにこの要素を使用する場合は、特に重要になります。

2. セーフティPLC

必要なロジックおよび計時機能を、対応する安全度水準で(セーフティ) PLCを使用することで簡単に実装することができます。実際には、これはSmartGuardまたはGuardLogixなどのセーフティPLCを使用して実現できます。

米国の安全制御システムの要件

米国には、安全関連の制御システム要件に関する多種多様な規格が存在しますが、特に有力な文書が、ANSI B11.TR3とANSI R15.06の2つです。技術レポートANSI B11.TR3では、期待されるリスク低減の規模によって分類される4つのレベルを定めています。各レベルの要件を以下に示します。

最低

最低限のリスク低減を実現するANSI B11.TR3安全ガードには、電気、電子、油圧、または空圧デバイスと、それに関連するシングルチャネル構成を使用する制御システムが含まれます。これらの要件の中で、安全定格デバイスの使用が絶対的な要件です。これは、ISO13849-1のカテゴリ1とほぼ同等です。

低/中レベルのリスク低減

低/中レベルのリスク低減を実現するANSI B11.TR3の安全ガードには、安全システムの性能を確認するために手動チェックが可能な冗長性を備えた制御システムが含まれます。要件に注目すると、システムは単純な冗長を採用します。チェック機能の使用は必須ではありません。チェックを行なわないと、冗長安全コンポーネントの一方が故障しても、安全システムがそれを認識しないことになります。これで、結果的にはシングル・チャネル・システムになります。このレベルのリスク低減は、チェック機能を使用した場合はカテゴリ2に最も近くなります。

高/中レベルのリスク低減

高/中レベルのリスク低減を実現するANSI B11.TR3の安全ガードには、安全システムの性能を確認するために始動時に自己チェックが可能な冗長性を備えた制御システムが含まれています。毎日起動するマシンの場合は、この自己チェック機能により、単なる冗長システムに比べ安全度水準が大幅に向上します。年中無休で稼働している機械の場合は、自己チェックはよくてもわずかな改善にすぎません。安全システムを定期的にモニタする機能を備えている場合は、カテゴリ3の要件と同等です。

最高のリスク低減

最高のリスク低減を提供するANSI B11.TR3の安全ガードには、連続自己チェック機能を行なう冗長性を備えた制御システムが含まれています。自己チェックで安全システムの性能を確認できなければなりません。安全システム設計者の大きな課題は、何を継続的と見なすかを明らかにすることです。ほとんどの安全システムは、始動時と安全システムに要求が出された時点でチェックを行ないます。

コンポーネントの中には連続自己チェックを実行するものもあります。例えば、ライトカーテンは、順次LEDが点灯と消灯を切換えます。ライトカーテンは連続自己チェックを行なっているため、フォルトが発生すると、安全システムに要求が出される前に出力をオフにします。マイクロプロセッサベースのリレーとセーフティPLCも、連続して自己チェックを行なうコンポーネントです。

「連続」自己チェック機能に関する制御システムの要件は、ライトカーテンやマイクロプロセッサベースのロジックユニット用のコンポーネントの選択肢を制限するものではありません。チェックは始動時および安全システムに要求が出された後に実行する必要があります。このレベルのリスク低減は、ISO13849-1のカテゴリ4と同程度です。

ロボット規格：米国およびカナダ

米国(ANSI RIA R15.06)およびカナダ(CSA Z434-03)のロボット規格は、ほとんど同じです。どちらにもEN954-1:1996のカテゴリと同様に4つのレベルがあり、以下に説明します。

単純

この最低レベルの「単純」では、安全制御システムは容認されたシングルチャネル回路を使用して設計・構成する必要があります。これらのシステムはプログラム可能な場合もあります。カナダでは、このレベルは信号と告知のみに限定されています。安全システムの設計者の大きな課題は、何を容認できると見なすかを明らかにすることです。容認できるシングルチャネル回路とは何なのでしょう? そのシステムはだれに容認されるのでしょうか? 単純なカテゴリは、EN954-1:1996のカテゴリBとほぼ同じです。

シングルチャネル

次のレベルは、以下のようなシングルチャネルの安全制御システムです。

- ハードウェアベースであるか、または安全定格ソフトウェア/ファームウェアデバイスであるか
- 安全定格のコンポーネントを含む。
- 製造メーカの推奨事項に従って使用する。
- 実績のある回路の設計を使用する。

実績のある回路設計の1例として、オフ状態で停止信号を送るシングルチャネルの電気機械式のポジティブ・ブレーク・デバイスがあります。シングル・チャネル・システムであると、1つのコンポーネントの故障が安全機能の損失につながる可能性があります。単純カテゴリは、EN9541:1996のカテゴリ1とほぼ同じです。

安全定格ソフトウェア/ファームウェアデバイス

ハードウェアベースのシステムにはロボットの安全ガードを実現する優先方法がありましたが、複雑なシステムに対応できることから、ソフトウェア/ファームウェアデバイスが選択されることが多くなってきました。ソフトウェア/ファームウェアデバイス(セーフティPLCおよびセーフティコントローラ)は、安全定格されていれば、使用することができます。この定格では、1つの安全定格コンポーネントまたはファームウェアの故障が安全機能の損失につながらないと定めています。フォルトが検出されると、その後のロボットの自動操作は、フォルトが解決されるまで抑制されます。

安全定格を満たすには、ソフトウェア/ファームウェアデバイスが認可基準を満たすことを認可された研究機関で検査する必要があります。米国では、OSHAが国家認定試験機関(NRTL)のリストを管理しています。カナダでは、カナダ規格審査会(SCC)が同様のリストを管理しています。

モニタ機能付きシングルチャネル

モニタ機能付きのシングルチャネル安全制御システムは、シングルチャネルに関する要件を満たし、安全定格され、チェック機能を利用している必要があります。安全機能のチェックは、機械の始動時と動作中に定期的に実行する必要があります。

チェック作業では、フォルトが検出されなければ運転を許可し、フォルトが検出された場合は停止信号を指令します。動作が停止された後も危険性が残っている場合は、警告を発します。当然ながら、チェック自体が危険な状態を引き起こすことは許されません。フォルトを検出した後は、そのフォルトが解決されるまで、ロボットは安全な状態を保つ必要があります。モニタ機能付きのシングルチャネルは、EN954-1:1996のカテゴリ2とほぼ同じです。

制御信頼性

米国およびカナダのロボット規格での最高レベルのリスク低減は、信頼できる制御の要件を満たす安全関連制御システムによって実現されます。制御信頼性の高い安全関連制御システムは、モニタ機能付きデュアル・チャネル・アーキテクチャです。ロボットの停止機能は、モニタ機能も含め、いかなる単一コンポーネントの障害によっても抑制されることは許されません。

モニタ機能は、フォルト検出時に停止コマンドを指令します。動作が停止した後も危険が残る場合は、警告信号を送る必要があります。安全システムは、フォルトが修正されるまで安全な状態を保つ必要があります。できれば、フォルトは障害が起きた時点で検出されることが望まれます。これが実現不可能な場合は、安全システムに次の要求が出された時点で障害が検出されなければなりません。同様の障害が発生する可能性が大きい場合は、コモンモード故障と考える必要があります。

カナダの要件には、米国の要件に2つの追加要件が加わります。1つは、安全関連制御システムが通常のプログラム制御システムから独立していることです。もう1つは、安全システムは気づかれることなく簡単に無効化されたり、バイパスされてはいけないということです。

制御信頼性システムは、EN 954-1:1996のカテゴリ3および4に相当します。

制御信頼性でのコメント

制御信頼性の最も基本的なものは、シングル・フォルト・トレランスです。要件として、単一フォルト、何らかの故障、または単一コンポーネントの故障が存在する場合に、安全システムはどのように対応すべきかを説明しています。

フォルトに関して、以下の3つの重要な概念を考慮する必要があります。

(1) すべてのフォルトが検出できるとは限らない。

(2) コンポーネントと言う言葉が加わると、配線の問題が発生する。

(3) 配線は安全システムに不可欠な要素であり、配線フォルトは安全機能の損失につながる。

制御信頼性の目的は、フォルトが存在するときに安全機能を実行することであるのは明らかです。フォルトが検出された場合、安全システムは安全措置を実行し、フォルトを通知して、フォルトが解決されるまで機械が動作を続けないようにする必要があります。フォルトが検出されなかった場合でも、要求があれば、安全機能を実行する必要があります。

SISTEMAを使用するアプリケーション例

このアプリケーション例には、2つのゾーンの安全システムをモニタするためにCompact GuardLogix PACとPointGuard IOを配線、構成、およびプログアムする方法を示します。各ゾーンには1つのセーフティ・インターロック・スイッチが含まれており、作動するとゾーンの冗長コンタクタのペアから電力の除去を通知します。これは、2番目のゾーンに複製されます。また、両方のゾーンはグローバルなE-stopで保護されており、作動時に両方のゾーンが安全にシャットダウンすることを示します。

注：この例は、説明のためにのみ示しています。多くの変数と要件は特定の取付けに関連しているため、ロックウェル･オートメーションではこの例に基づいた実際の使用について責任を負うことはできません。

特長および利点

- Compact GuardLogixでは、標準と安全の両方のアプリケーションを1台のコントローラで実行できる。
- 標準および安全I/Oは、1つのEthernetアダプタで組み合わせることができる。
- 安全ステータスと診断は、HMIで表示するために安全アプリケーションから標準アプリケーションに簡単に渡すことができ、Ethernet上の追加デバイスにリモートで渡すことができ。
- ここに説明するアプリケーションは拡張でき、カスタマアプリケーションに組込むことができる。

説明

このアプリケーションは2つのゾーンをモニタします。各ゾーンは、SensaGuardセーフティスイッチで保護されています。いずれかのゲートが開くと、出力コンタクタがオフして、そのゾーンの関連するマシンがシャットダウンします。リセットは手動です。また、両方のゾーンはグローバルなE-stopスイッチで保護されています。E-stopが作動すると、コンタクタの両方のセットがオフします。

安全機能

各SensaGuardセーフティスイッチは、1734-IB8Sモジュール(POINTGuard I/O)の安全入力のペアに接続されます。I/Oモジュールは、EtherNet/IPネットワークのCIP SafetyをCompact GuardLogixセーフティコントローラ(1768-L43S)に接続されます。セーフティプロセッサの安全コードは、デュアルチャネル入力停止(DCS)という名前の認可済みの安全命令を使用する安全入力のステータスをモニタします。安全コードは、1oo2プロセッサ構成で並列に実行します。すべての条件が満たされると、セーフティゲートが閉じて、入力モジュールでフォルトが検出されず、グローバルなE-stopは作動せず、リセット押しボタンを押して、構成可能な冗長出力(CROUT)という2番目の認可ファンクションブロックが、最終的な制御デバイスである100S冗長コンタクタのペアのステータスをチェックします。コントローラは出力信号を1734-OBSモジュールに送って、ON出力のペアを切換えてセーフティコンタクタをオンします。また、グローバルなE-stop機能もDCS命令によってモニタされます。グローバルなE-stopが作動すると、両方のゾーンがシャットダウンします。

部品表

このアプリケーション例では、以下のコンポーネントを使用しています。

Cat.No.	説明	数量
440N-Z21SS2A	SensaGuardスイッチ、非接触型プラスチックRFP	2
800FM-G611MX10	800Fリセット押しボタン - 金属製、ガード付き、青色、R、金属製のラッチ取付け、1 N.O.接点、標準	4
100S-C09ZJ23C	Bulletin 100S-C - セーフティコンタクタ	2
1768-ENBT	CompactLogix EtherNet/IPブリッジモジュール	1
1768-L43S	CompactLogix L43プロセッサ、2.0 MB標準メモリ、0.5 MB安全メモリ	1
1768-PA3	電源AC120/240V入力、DC24Vのとき3.5A	1
1769-ECR	右のエンドキャップ/終端抵抗	1
1734-AENT	DC24V Ethernetアダプタ	1
1734-TB	取り外し可能なIECねじ端子付きモジュールベース	4
1734-IB8S	安全入力モジュール	2
1734-OB8S	安全出力モジュール	1
1783-US05T	Stratix 2000非管理型Ethernetスイッチ	1

セットアップおよび配線

取付けと配線の詳細は、製品に付属するマニュアルか、または以下のWebサイトからダウンロードできるマニュアルを参照してください：
http://literature.rockwellautomation.com

システム概要

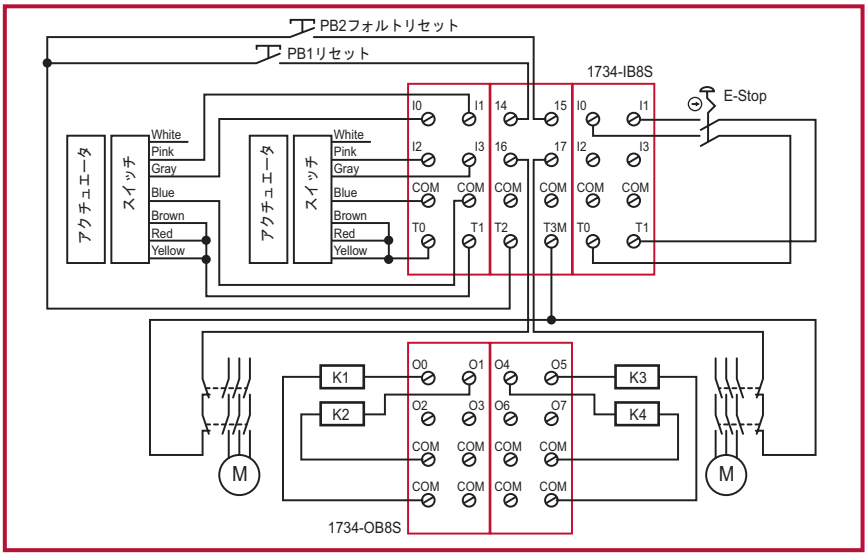
1734-IB8S入力モジュールは、両方のSensaGuardスイッチからの入力をモニタします。

Sensaguardは、出力の周期的にテストを実施するOSSD出力を使用します。このため、SensaGuardスイッチと安全入力間の配線の整合性をテストするOSSD出力です。

テストパルス出力は、24V電源として構成されます。

最終的な制御デバイスは、100SセーフティコンタクタのペアであるK1とK2です。コンタクタは、1734-OBS安全出力モジュールによって制御されます。これらは、冗長構成に配線され、始動時にフォルトについてテストします。始動テストは、コンタクタがオンする前に入力2 (I2)へのフィードバック回路をモニタすることで行なわれます。これは、構成可能な冗長出出力(CROUT)命令を使用して行なうことができます。システムはモメンタリ式押しボタンであるPB1でリセットされます。

配線



Allen-Bradley

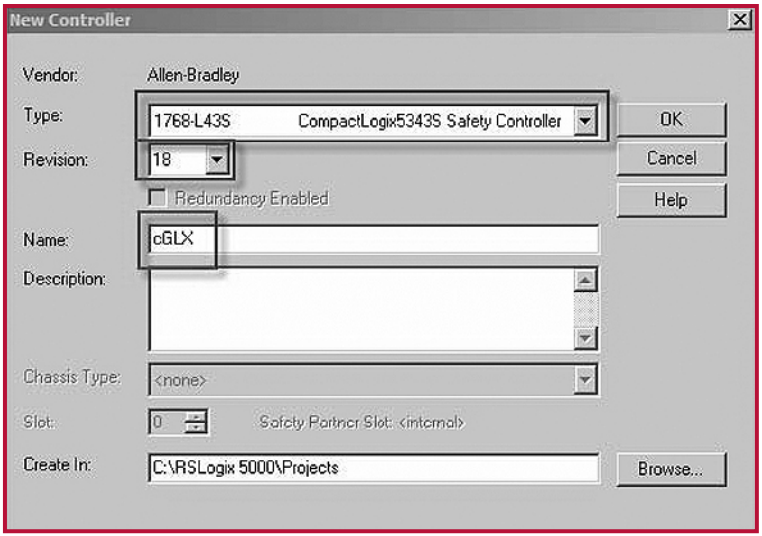
構成

Compact GuardLogixコントローラは、RSLogix 5000, Ver. 18以降を使用して構成できます。新しいプロジェクトを作成してから、I/Oモジュールを追加する必要があります。それから、適切な入力と出力タイプについてI/Oモジュールを構成します。各ステップの詳細な説明は、本書の範囲を超えています。RSLogixプログラミング環境についての知識があることを前提としています。

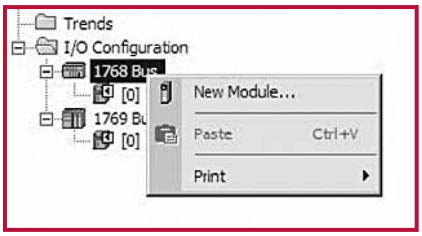
コントローラの構成およびI/Oモジュールの追加

以下の手順を行なってください。

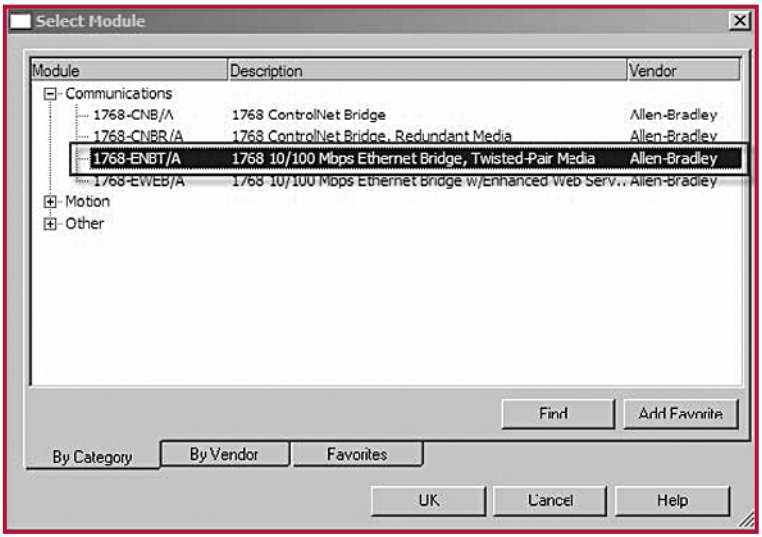
1. RSLogix 5000ソフトウェアで、新しいプロジェクトを作成します。



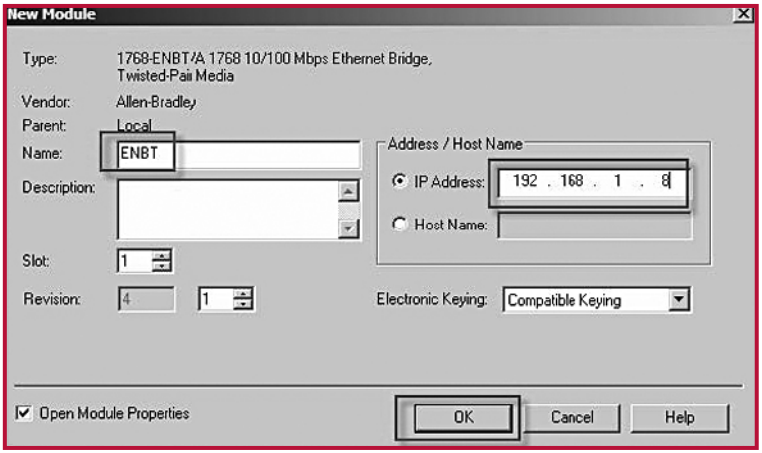
2. コントローラオーガナイザで、1768-ENBTモジュールを1768バスに追加します。



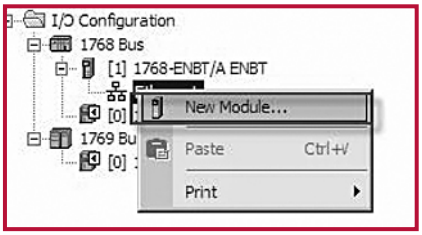
3. 1768-ENBTモジュールを選択してから、OKをクリックします。



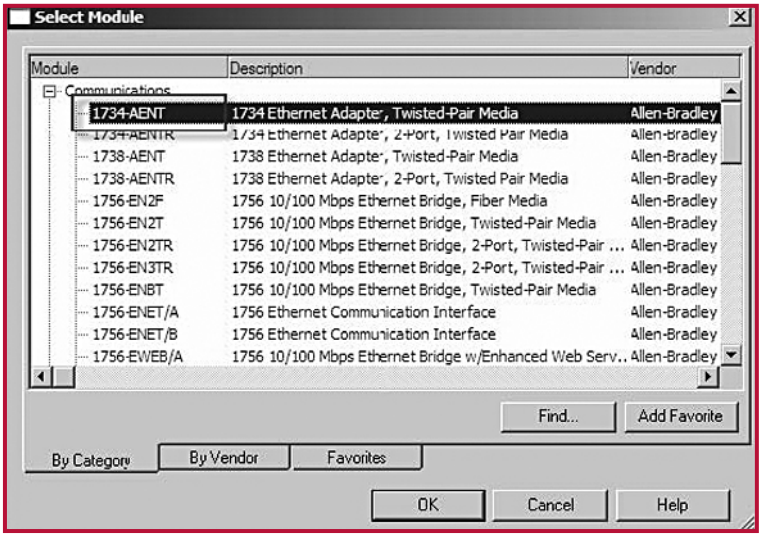
4. モジュールの名前を指定して、IPアドレスを入力してからOKをクリックします。このアプリケーション例では192.168.1.8 を使用しています。異なる設定も可能です。



5. コントローラオーガナイザで1768-ENBTモジュールを右クリックしてからNew Moduleを選択することで、1734-AENTアダプタを追加します。

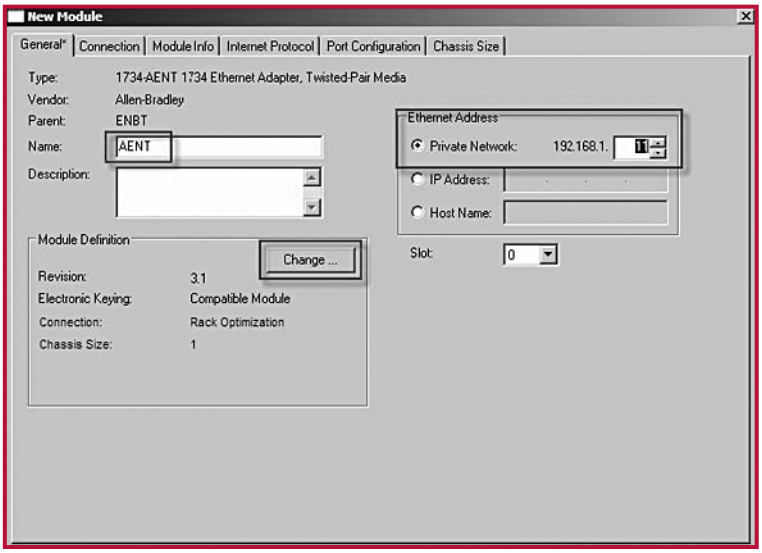


6. 1734-AENTアダプタを選択してから、OKをクリックします。



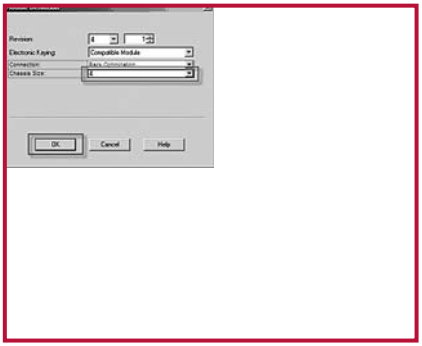
7. モジュールの名前を指定して、IPアドレスを入力してからOKをクリックします。このアプリケーション例では192.168.1.11を使用しています。異なる設定も可能です。

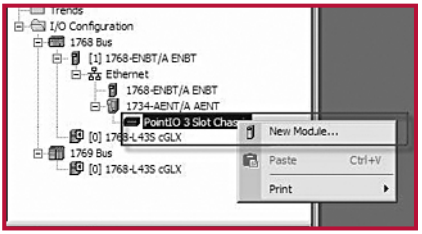
8. Changeをクリックします。



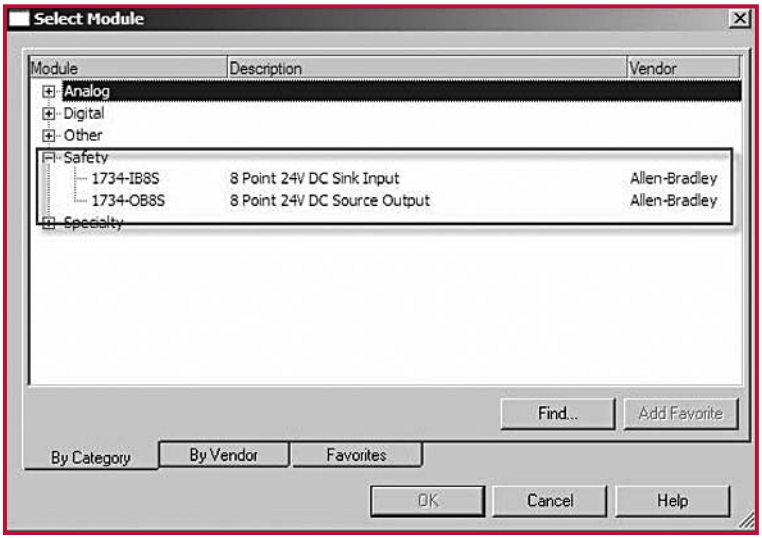
9. Chassis Size (シャーシサイズ)を1734-AENTアダプタ用に4を設定してから、OKをクリックします。シャーシサイズは、シャーシに挿入されるモジュール数です。1734-AENTアダプタはスロット0にあると考えられるため、2つの入力モジュールと1つの出力モジュールで、シャーシサイズは4です。

10. コントローラオーガナイザで、1734-AENTアダプタを右クリックしてからNew Moduleを選択します。

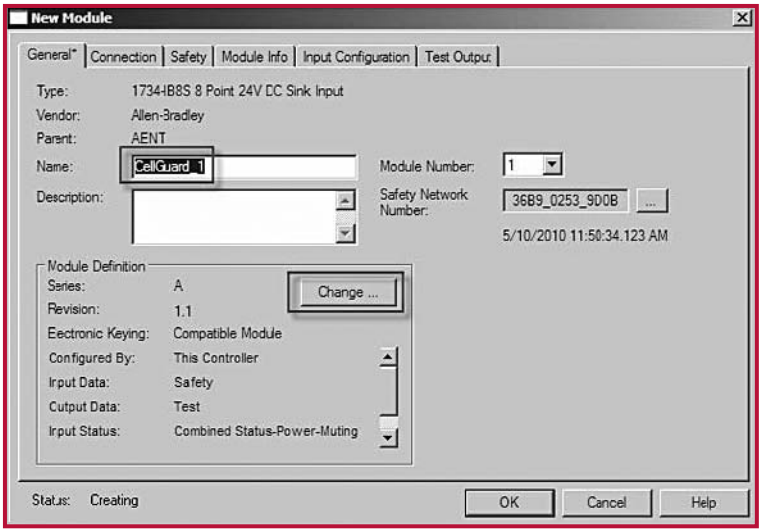




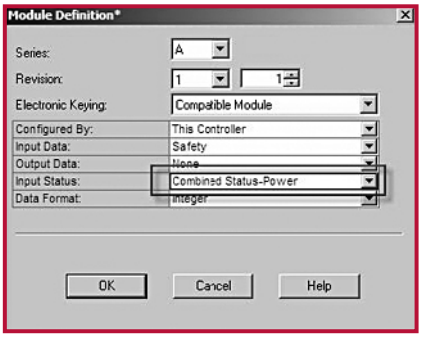
11. Safetyを展開して、1734-IB8Sモジュールを選択してからOKをクリックします。



12. New Moduleダイアログボックスで、デバイスの名前として‘CellGuard_1’を指定してから、Changeをクリックします。



13. Module Definitionダイアログボックスを開いて、Input StatusをCombined Status-Powerに変更してから、OKをクリックします。



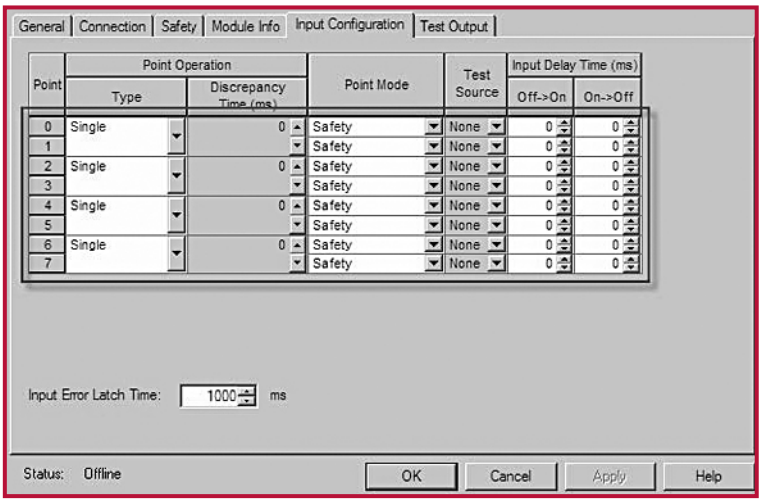
14. OKをクリックすることで、Module Propertiesダイアログボックスを閉じます。

15. ステップ10～14を繰返して、2番目の1734-IB8S安全入力モジュールと1734-OB8S安全出力モジュールを追加します。

I/Oモジュールの構成

以下の手順に従って、POINT Guard I/Oモジュ0ルを構成してください。

1. コントローラオーガナイザで、1734-IB8Sモジュールを右クリックしてからPropertiesを選択します。
2. Input Configurationをクリックして、以下に示すようにモジュールを構成します。



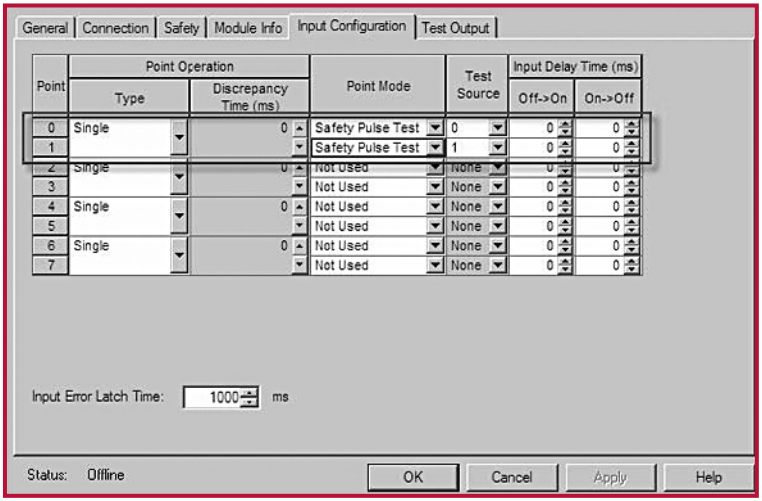
Allen-Bradley

3. Test Outputをクリックしてから、以下に示すようにモジュールを構成します。

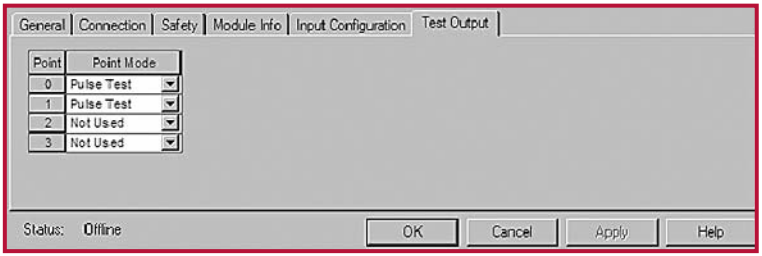
4. OKをクリックします。

5. コントローラオーガナイザで、2番目の1734-IB8Sモジュールを右クリックしてからPropertiesを選択します。

6. Input Configurationをクリックして、以下に示すようにモジュールを構成します。



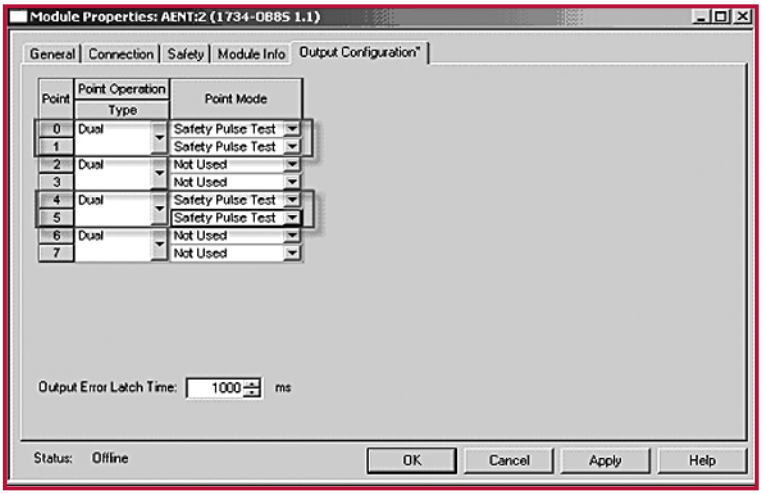
7. Test Outputをクリックしてから、以下に示すようにモジュールを構成します。



8. OKをクリックします。

9. コントローラオーガナイザで、1734-OB8Sモジュールを右クリックしてからPropertiesを選択します。

10. Output Configurationをクリックしてから、以下に示すようにモジュールを構成します。

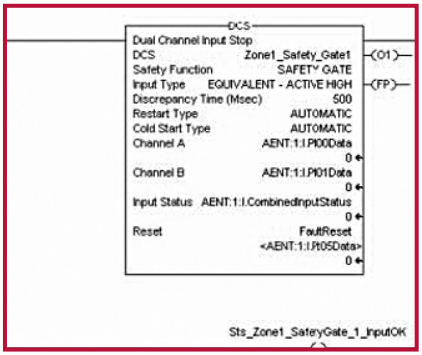


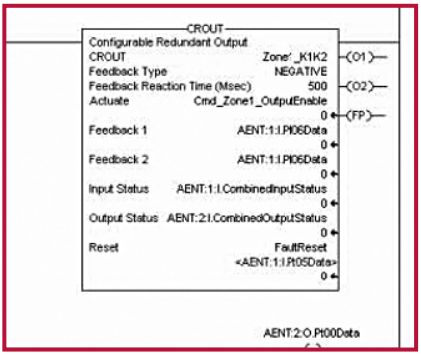
11. OKをクリックします。

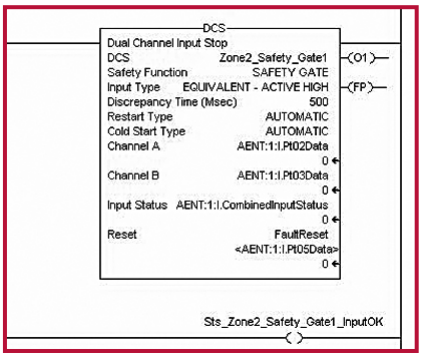
プログラミング

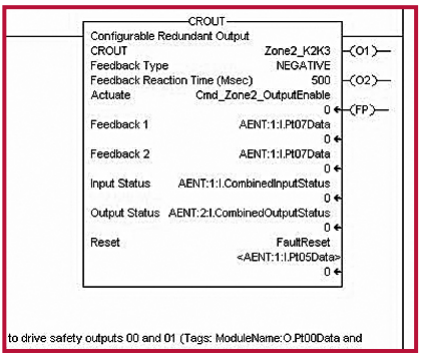
デュアルチャネル入力停止(DCS)命令は、デュアル入力安全デバイスをモニタします。その主な機能はマシンが安全に停止することです(例えば、E-stop、ライトカーテン、またはセーフティゲート)。この命令は、両方の安全入力が(Channel AとChannel B)がInput Typeパラメータで判断されるようにアクティブ状態で、適切なリセット動作が実施されたときのみ、Output 1をオンにできます。DCS命令は、整合性についてデュアル入力チャネルをモニタし(Equivalent - Active High)、構成されたディスクレパンシ時間(単位：msec)の間に不一致が検出されるとフォルトを検出して補足します。構成可能な冗長出力(CROUT)命令は、冗長出力を制御およびモニタします。出力フィードバックの応答時間は構成可能です。命令は、ポジティブ(正)とネガティブ(負)のフィードバック信号をサポートしています。

安全出力ルーチン内の安全アプリケーションコードは、入力チャネルが自動的にリセットすると、回路リセットのために反タイダウン機能を提供して、出力が再起動するのを防止します。



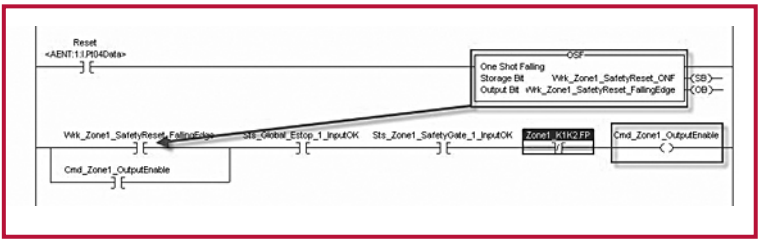






立下り時リセット

EN ISO 13849-1では、リセット命令の機能が立下り時信号で起こらなければならないことを規定しています。この要件を満たすには、以下に示すようにリセットコードに立下り時ワンショット命令を追加します。



性能データ

適切に構成された場合は、各安全機能はEN ISO 13849.1 2008に従うPLe、カテゴリ4の安全定格を達成できます。

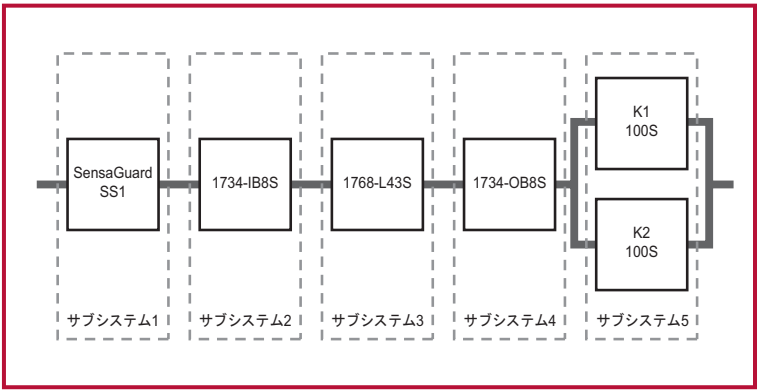
1年が360日で1日16時間稼動して、セーフティゲートが1時間ごとに1回動作するとして計算されるため、1年間に合計5760回動作することなります。グローバルなE-stop機能は、1ヶ月に1回テストされます。

Estop 1	
PLr	d
PL	e
PFH [1/h]	5E-8

Estop 1	
PLr	d
PL	e
PFH [1/h]	5E-8

Safety Gate 2	
PLr	e
PL	e
PFH [1/h]	2.64E-8

各セーフティゲート機能は、以下のように表すことができます。



SB Interlock Switch: SensaGuard	
PL	e
PFH [1/h]	1.12E-9
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

SB Safety I/O: 1734-IB8S	
PL	e
PFH [1/h]	2.25E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

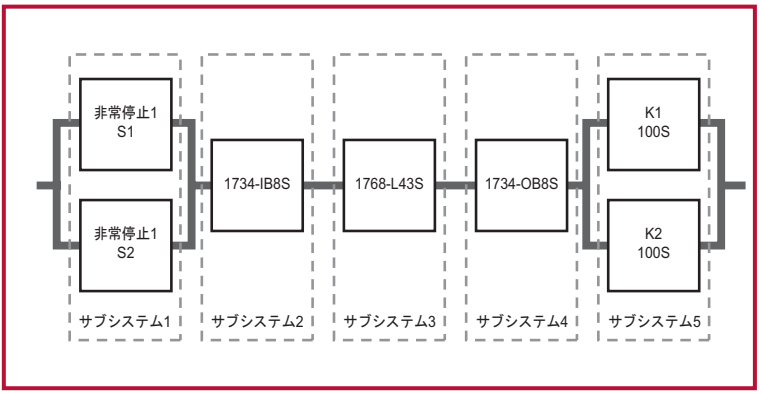
SB Safety PLC: Compact GuardLogix 1768	
PL	e
PFH [1/h]	2.1E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

SB Safety I/O: 1734-OB8S	
PL	e
PFH [1/h]	2.29E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

SB Contactors	
PL	e
PFH [1/h]	2.47E-8
Cat.	4
MTTFd [a]	100 (High)
DCavg [%]	99 (High)
CCF	65 (fulfilled)

SISTEMAを使用するアプリケーション例

E-stop機能は、以下のように表すことができます。



SB Estop 1	
PL	e
PFH [1/h]	2.47E-8
Cat.	4
MTTFd [a]	100 (High)
DCavg [%]	99 (High)
CCF	65 (fulfilled)

SB Safety I/O: 1734-IB8S	
PL	e
PFH [1/h]	2.25E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

SB Safety PLC: Compact GuardLogix 1768	
PL	e
PFH [1/h]	2.1E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

SB Safety I/O: 1734-OB8S	
PL	e
PFH [1/h]	2.29E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

SB Contactors	
PL	e
PFH [1/h]	2.47E-8
Cat.	4
MTTFd [a]	100 (High)
DCavg [%]	99 (High)
CCF	65 (fulfilled)

この例では、SISTEMA計算ファイルおよびRSLogix 5000アプリケーションコードを以下のWebサイトからダウンロードできます：
www.discoverrockwellautomation.com

この例に使用されている製品の詳細は、ロックウェル･オートメーションの literature library (リタレチャライブラリ)を参照して、以下にボールド体で示す Pub.No.を検索してください。また、一般的な製品の概要については、www.ab.comをご覧ください。

リタレチャライブラリのアドレス：**www.theautomationbookstore.com**

マニュアル名	説明
Compact GuardLogix Controllers User Manual (Compact GuardLogixコントローラ ユーザーズマニュアル) Pub.No.: **1768-UM002**	Compact GuardLogixコントローラの取付け、構成、操作、および保守について説明する。
POINT Guard I/O Safety Modules Installation and User Manual (POINT Guard I/O Safetyモジュール インストレーション&ユーザーズマニュアル) Pub.No.: **1734-UM013**	POINT Guard I/Oモジュールの取付け、構成、および操作について説明する。
GuardLogix Controller Systems Safety Reference Manual (GuardLogixコントローラシステム セーフティ・リファレンス・マニュアル) Pub.No.: **1756-RM093**	GuardLogixコントローラシステムの安全定格を達成して、保持するための詳細な要件
GuardLogix Safety Application Instruction Set Reference Manual (GuardLogix安全アプリケーション・インストラクション・セット セーフティ・リファレンス・マニュアル) Pub.No.: **1756-RM095**	GuardLogix安全アプリケーションの命令セットについて、詳細に説明する。
Safety Accelerator Toolkit for GuardLogix Systems Quick Start Guide (GuardLogixシステム用の Safety Accelerator Toolkit クイックスタート) Pub.No.: **IASIMP-QS005**	Safety Accelerator Toolkitでの設計、プログラミング、および診断ツールを使用するための段階的に説明したガイド
Safety Products Calatogue (セーフティ製品カタログ) Publ.No.: **S117-CA001A**	セーフティ製品、アプリケーション例、および有用な情報を含む総合的な資料

ロックウェル･オートメーションは、リタレチャライブラリからダウンロード可能な同様の例のセットを開発しています。リタレチャライブラリにアクセスして、ドロップダウンメニューで ‘Publication Number’ を選択してから、検索フィールドに ‘SAFETY-AT’ を入力して検索を実行してください。

SISTEMA計算およびRSLogix 5000 アプリケーションコードはアプリケーションの一部で使用でき、以下のWebサイトからダウンロードできます：
www.discoverrockwellautomation.com

SISTEMAを使用するアプリケーション例

各チャネルのMTTFd年	時間単位当たりの危険側故障の平均割合(1/h)と対応する安全遂行レベル(PL)													
	Cat. B	PL	Cat. 1	PL	Cat. 2	PL	Cat. 2	PL	Cat. 3	PL	Cat. 3	PL	Cat. 4	PL
	DC_{avg} = なし		DC_{avg} = なし		DC_{avg} = 低		DC_{avg} = 中		DC_{avg} = 低		DC_{avg} = 中		DC_{avg} = 高	
3	$3{,}80 \times 10^{-5}$	a			$2{,}58 \times 10^{-5}$	a	$1{,}99 \times 10^{-5}$	A	$1{,}26 \times 10^{-5}$	a	$6{,}09 \times 10^{-6}$	b		
3,3	$3{,}46 \times 10^{-5}$	a			$2{,}33 \times 10^{-5}$	a	$1{,}79 \times 10^{-5}$	A	$1{,}13 \times 10^{-5}$	a	$5{,}41 \times 10^{-6}$	b		
3,6	$3{,}17 \times 10^{-5}$	a			$2{,}13 \times 10^{-5}$	a	$1{,}62 \times 10^{-5}$	a	$1{,}03 \times 10^{-5}$	a	$4{,}86 \times 10^{-6}$	b		
3,9	$2{,}93 \times 10^{-5}$	a			$1{,}95 \times 10^{-5}$	a	$1{,}48 \times 10^{-5}$	a	$9{,}37 \times 10^{-6}$	b	$4{,}40 \times 10^{-6}$	b		
4,3	$2{,}65 \times 10^{-5}$	a			$1{,}76 \times 10^{-5}$	a	$1{,}33 \times 10^{-5}$	a	$8{,}39 \times 10^{-6}$	b	$3{,}89 \times 10^{-6}$	b		
4,7	$2{,}43 \times 10^{-5}$	a			$1{,}60 \times 10^{-5}$	a	$1{,}20 \times 10^{-5}$	a	$7{,}58 \times 10^{-6}$	b	$3{,}48 \times 10^{-6}$	b		
5,1	$2{,}24 \times 10^{-5}$	a			$1{,}47 \times 10^{-5}$	a	$1{,}10 \times 10^{-5}$	a	$6{,}91 \times 10^{-6}$	b	$3{,}15 \times 10^{-6}$	b		
5,6	$2{,}04 \times 10^{-5}$	a			$1{,}33 \times 10^{-5}$	a	$9{,}87 \times 10^{-6}$	b	$6{,}21 \times 10^{-6}$	b	$2{,}80 \times 10^{-6}$	c		
6,2	$1{,}84 \times 10^{-5}$	a			$1{,}19 \times 10^{-5}$	a	$8{,}80 \times 10^{-6}$	b	$5{,}53 \times 10^{-6}$	b	$2{,}47 \times 10^{-6}$	c		
6,8	$1{,}68 \times 10^{-5}$	a			$1{,}08 \times 10^{-5}$	a	$7{,}93 \times 10^{-6}$	b	$4{,}98 \times 10^{-6}$	b	$2{,}20 \times 10^{-6}$	c		
7,5	$1{,}52 \times 10^{-5}$	a			$9{,}75 \times 10^{-6}$	b	$7{,}10 \times 10^{-6}$	b	$4{,}45 \times 10^{-6}$	b	$1{,}95 \times 10^{-6}$	c		
8,2	$1{,}39 \times 10^{-5}$	a			$8{,}87 \times 10^{-6}$	b	$6{,}43 \times 10^{-6}$	b	$4{,}02 \times 10^{-6}$	b	$1{,}74 \times 10^{-6}$	c		
9,1	$1{,}25 \times 10^{-5}$	a			$7{,}94 \times 10^{-6}$	b	$5{,}71 \times 10^{-6}$	b	$3{,}57 \times 10^{-6}$	b	$1{,}53 \times 10^{-6}$	c		
10	$1{,}14 \times 10^{-5}$	a			$7{,}18 \times 10^{-6}$	b	$5{,}14 \times 10^{-6}$	b	$3{,}21 \times 10^{-6}$	b	$1{,}36 \times 10^{-6}$	c		
11	$1{,}04 \times 10^{-5}$	a			$6{,}44 \times 10^{-6}$	b	$4{,}53 \times 10^{-6}$	b	$2{,}81 \times 10^{-6}$	c	$1{,}18 \times 10^{-6}$	c		
12	$9{,}51 \times 10^{-5}$	b			$5{,}84 \times 10^{-6}$	b	$4{,}04 \times 10^{-6}$	b	$2{,}49 \times 10^{-6}$	c	$1{,}04 \times 10^{-6}$	c		
13	$8{,}78 \times 10^{-5}$	b			$5{,}33 \times 10^{-6}$	b	$3{,}64 \times 10^{-6}$	b	$2{,}23 \times 10^{-6}$	c	$9{,}21 \times 10^{-7}$	d		
15	$7{,}61 \times 10^{-6}$	b			$4{,}53 \times 10^{-6}$	b	$3{,}01 \times 10^{-6}$	b	$1{,}82 \times 10^{-6}$	c	$7{,}44 \times 10^{-7}$	d		
16	$7{,}31 \times 10^{-6}$	b			$4{,}21 \times 10^{-6}$	b	$2{,}77 \times 10^{-6}$	c	$1{,}67 \times 10^{-6}$	c	$6{,}76 \times 10^{-7}$	d		

各チャネルのMTTFd年	時間単位当たりの危険側故障の平均割合(1/h)と対応する安全遂行レベル(PL)													
	Cat. B	PL	Cat. 1	PL	Cat. 2	PL	Cat. 2	PL	Cat. 3	PL	Cat. 3	PL	Cat. 4	PL
	DC_{avg} = なし		DC_{avg} = なし		DC_{avg} = 低		DC_{avg} = 中		DC_{avg} = 低		DC_{avg} = 中		DC_{avg} = 高	
18	$6{,}34 \times 10^{-6}$	b			$3{,}68 \times 10^{-6}$	b	$2{,}37 \times 10^{-6}$	c	$1{,}41 \times 10^{-6}$	c	$5{,}67 \times 10^{-7}$	d		
20	$5{,}71 \times 10^{-6}$	b			$3{,}26 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}22 \times 10^{-6}$	c	$4{,}85 \times 10^{-7}$	d		
22	$5{,}19 \times 10^{-6}$	b			$2{,}93 \times 10^{-6}$	c	$1{,}82 \times 10^{-6}$	c	$1{,}07 \times 10^{-6}$	c	$4{,}21 \times 10^{-7}$	d		
24	$4{,}76 \times 10^{-6}$	b			$2{,}65 \times 10^{-6}$	c	$1{,}62 \times 10^{-6}$	c	$9{,}47 \times 10^{-7}$	d	$3{,}70 \times 10^{-7}$	d		
27	$4{,}23 \times 10^{-6}$	b			$2{,}32 \times 10^{-6}$	c	$1{,}39 \times 10^{-6}$	c	$8{,}04 \times 10^{-7}$	d	$3{,}10 \times 10^{-7}$	d		
30			$3{,}80 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}21 \times 10^{-6}$	c	$6{,}94 \times 10^{-7}$	d	$2{,}65 \times 10^{-7}$	d	$9{,}54 \times 10^{-8}$	e
33			$3{,}46 \times 10^{-6}$	b	$1{,}85 \times 10^{-6}$	c	$1{,}06 \times 10^{-6}$	c	$5{,}94 \times 10^{-7}$	d	$2{,}30 \times 10^{-7}$	d	$8{,}57 \times 10^{-8}$	e
36			$3{,}17 \times 10^{-6}$	b	$1{,}67 \times 10^{-6}$	c	$9{,}39 \times 10^{-7}$	d	$5{,}16 \times 10^{-7}$	d	$2{,}01 \times 10^{-7}$	d	$7{,}77 \times 10^{-8}$	e
39			$2{,}93 \times 10^{-6}$	c	$1{,}53 \times 10^{-6}$	c	$8{,}40 \times 10^{-7}$	d	$4{,}53 \times 10^{-7}$	d	$1{,}78 \times 10^{-7}$	d	$7{,}11 \times 10^{-8}$	e
43			$2{,}65 \times 10^{-6}$	c	$1{,}37 \times 10^{-6}$	c	$7{,}34 \times 10^{-7}$	d	$3{,}87 \times 10^{-7}$	d	$1{,}54 \times 10^{-7}$	d	$6{,}37 \times 10^{-8}$	e
47			$2{,}43 \times 10^{-6}$	c	$1{,}24 \times 10^{-6}$	c	$6{,}49 \times 10^{-7}$	d	$3{,}35 \times 10^{-7}$	d	$1{,}34 \times 10^{-7}$	d	$5{,}76 \times 10^{-8}$	e
51			$2{,}24 \times 10^{-6}$	c	$1{,}13 \times 10^{-6}$	c	$5{,}80 \times 10^{-7}$	d	$2{,}93 \times 10^{-7}$	d	$1{,}19 \times 10^{-7}$	d	$5{,}26 \times 10^{-8}$	e
56			$2{,}04 \times 10^{-6}$	c	$1{,}02 \times 10^{-6}$	c	$5{,}10 \times 10^{-7}$	d	$2{,}52 \times 10^{-7}$	d	$1{,}03 \times 10^{-7}$	d	$4{,}73 \times 10^{-8}$	e
62			$1{,}84 \times 10^{-6}$	c	$9{,}06 \times 10^{-7}$	d	$4{,}43 \times 10^{-7}$	d	$2{,}13 \times 10^{-7}$	d	$8{,}84 \times 10^{-8}$	e	$4{,}22 \times 10^{-8}$	e
68			$1{,}68 \times 10^{-6}$	c	$8{,}17 \times 10^{-7}$	d	$3{,}90 \times 10^{-7}$	d	$1{,}84 \times 10^{-7}$	d	$7{,}68 \times 10^{-8}$	e	$3{,}80 \times 10^{-8}$	e
75			$1{,}52 \times 10^{-6}$	c	$7{,}31 \times 10^{-7}$	d	$3{,}40 \times 10^{-7}$	d	$1{,}57 \times 10^{-7}$	d	$6{,}62 \times 10^{-8}$	e	$3{,}41 \times 10^{-8}$	e
82			$1{,}39 \times 10^{-6}$	c	$6{,}61 \times 10^{-7}$	d	$3{,}01 \times 10^{-7}$	d	$1{,}35 \times 10^{-7}$	d	$5{,}79 \times 10^{-8}$	e	$3{,}08 \times 10^{-8}$	e
91			$1{,}25 \times 10^{-6}$	c	$5{,}88 \times 10^{-7}$	d	$2{,}61 \times 10^{-7}$	d	$1{,}14 \times 10^{-7}$	d	$4{,}94 \times 10^{-8}$	e	$2{,}74 \times 10^{-8}$	e
100			$1{,}14 \times 10^{-6}$	c	$5{,}28 \times 10^{-7}$	d	$2{,}29 \times 10^{-7}$	d	$1{,}01 \times 10^{-7}$	d	$4{,}29 \times 10^{-8}$	e	$2{,}47 \times 10^{-8}$	e

SAFEBOOK 4 - マシンの安全関連制御システム　原理、規格、および実装

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication Number SAFEBK-RM002B-JA-P —March 2011
© 2011 Rockwell Automation, Inc. All Rights Reserved.
Superceedes Publication: SAFEBK-RM002A-EN-P